



Security Management System, Version 5.3

User Manual



Ingersoll Rand Copyright Notice

© 2010 Ingersoll-Rand Company

This documentation and the software/hardware described herein, is furnished under license and may be used only in accordance with the terms of such license. Information contained in this manual is subject to change without notice and does not represent any commitment on the part of Ingersoll Rand. Ingersoll Rand assumes no responsibility or liability for any errors or inaccuracies that may appear in this documentation.

CONTACT INFORMATION

Schlage
Electronic Security
575 Birch Street
Forestville, CT 06010
Phone: 860-584-9158
Fax: 860-584-2136
www.schlage.com

To contact a local Ingersoll Rand Security Technologies Consultant in your area go to:
<http://securitytechnologies.ingersollrand.com/ssc.asp>

Contents

Ingersoll Rand Copyright Notice	1
<hr/>	
Typographical Conventions	21
<hr/>	
Acronym	22
<hr/>	
Preface	23
<hr/>	
Introduction	23
System Overview	23
Areas, cardholders and readers	23
Grouping Structure - Area Sets and Cardholder Categories	23
Area Access	24
Credentials	24
Transactions	24
Online and Offline Access Control	25
Schlage SMS Levels	27
<hr/>	
Installation and Getting Started	29
<hr/>	
Introduction	29
Operator's requirements	29
Minimum PC requirements	29
Installation instructions	30
Notes on Windows Vista/Windows 7 Install	37
Upgrade instructions	38
Guest Pass System Installation (only applicable to Schlage SMS Premier users)	41
System Launcher	42
Creating Launcher Groups	42
Default user ID and password	43
Adding applications to the Launcher Group	43
Deleting applications from user created groups	44
Renaming a Launcher Group	44
Arranging the icons of a Group	44

Icon - Views	44
Launcher Group Properties.....	45
Rearranging Launcher Group tabs.....	46
Recently Launched Applications	46
Exiting Launcher	46
Logging out of the system.....	47
Customer support.....	47
Hours of operation	47

Registry Editor 48

Introduction	48
Accessing the application.....	48
Settings	48
System Information	49
System Processes	50
Database Connection	51
Report Database Connection.....	52

System Settings 53

Introduction	53
Accessing the application.....	53
General Settings	54
Expiration Indicators	54
Default Programs and Devices	55
Backup Options.....	55
Cardholder Definition Default Expiration Date	55
Schlage SMS Image Settings.....	56
Image Handling.....	56
General Image Capture Settings.....	57
Schlage SMS Signature Settings	58
Online Credential Options and Pin Calculator.....	59
Enrollment Reader Setting.....	59
Advanced Search Settings.....	60
Credential Issuance Settings	60
Pin Calculator Settings.....	61

Area States and Door Types	62
Badge Printing Defaults	63
Badge Default Print Options	63
Dossier Default Print Options.....	63
Default Printers	64
Default Queues	64
Campus Lock Settings	65
Global Settings.....	65
Current Workstation Settings	67
Offline Credential Settings	68
Global Offline Credential Settings.....	68
Current Workstation Offline Credential Settings.....	71

System Manager 72

Introduction	72
Accessing the application.....	72
Working with System Manager.....	73
Overview.....	73
Timezone Intervals.....	74
Areas and Area Sets.....	75
Holidays and Holiday Sets	82
Lockdowns.....	83
Cardholder Categories.....	84
Callback Numbers and Callback Sets.....	85
Site Codes and Site Code Sets	85
Hardware Definitions.....	86
Magstripe Template Definition	130
Device Status.....	132
Editing records.....	133
View	134
Search	134

Cardholder Definition 137

Introduction	137
Accessing the application.....	137
Working with Cardholder Definition	138
Add a new Cardholder	138

Credential Definition.....	144
Connecting the hardware and determining the COM Port	145
Setting up the Enrollment Reader in Schlage SMS.....	145
Retire Credentials	167
Massive access control modification for cardholders	168
Add a new Cardholder (Method 2)	169
Duplicate Cardholder Information	169
Delete Cardholders	170
Exporting Cardholder Portraits.....	171
Printing Dossier Reports	172
View	172
Cardholder Search.....	174

Card Format Editor 180

Introduction	180
Accessing the application.....	180
Overview	180
Card Format Editor main window.....	181
Setting up Schlage Enrollment Reader	182
Connecting the hardware and determining the COM Port	182
Setting up the Enrollment Reader in Schlage SMS.....	183
Magstripe Template	184
Card Format Editor usage scenarios.....	184
Identifying existing credential formats	185
Editing Card Formats	188
Defining a new Magstripe Format	189
Adding a Card Format in the System	192
Defining a Wiegand Format.....	193
Add Card Formats in the System	193

System Security 194

Introduction	194
Accessing the application.....	194
Schlage SMS Select System Security.....	195
Working with System Security.....	196
Overview	196
Adding Security Groups	197

Define Launcher Items.....	202
Assigning security privileges	204

Badge Creation 215

Introduction	215
Accessing the application.....	215
Defining a new badge layout.....	216
Editing a Badge Layout.....	218
Duplicating a Badge Layout	218
Editing Magstripe Options.....	218
Defining annotations for a new Badge Layout	218
Editing Annotations	225
Importing and Exporting Badge Layouts	227

Badge Queue 230

Introduction	230
Accessing the application.....	230
Working with Badge Queue.....	230
Badge Queue Definition.....	231
File menu options.....	231
Adding cardholder Badges to the Queue	232
Printing Badges.....	232
Editing Queues	233
Viewing a Badge Layout	233
Search for Badge Queues	233
Advanced Find.....	234

User Defined Fields 235

Introduction	235
Accessing the application.....	235
Working with UDF Editor.....	235
Creating a new User Definable Field	236
Edit Options	242

E-mail Address Editor 243

Introduction	243
Accessing the application.....	243
Adding e-mail addresses.....	243
Mass Insert	244
Editing records.....	244
Deleting records.....	244
Search	244

UDF Cross Reference 246

Introduction	246
Accessing the application.....	246
Working with UDF Cross Reference	246
Before you begin.....	246
Mapping	247
Editing an Existing Mapping.....	249

Two Person Rule 250

Area Definition.....	250
Define Readers	251
Team Definition	252
Creating a Shift	253
Area Count Tracking	256
Define a Two Person Area - Schedules or Team.....	256
Supervisor Access	257

Portrait Monitor-Settings 258

Introduction	258
Overview	258
Accessing the Application	258
Configuring a Portrait Monitor Workstation.....	259
Portrait Monitor Search Wizard	259
Advanced Find.....	260

Portrait Monitor 261

Introduction	261
Starting the Portrait Monitor	261
Working with Portrait Monitor	262
Launching the Portrait Monitor	262
Detail View	262
Access Denied Transactions	263
Pausing Transactions	263
Manual Overrides within Portrait Monitor	263

Alarm Definition 264

Introduction	264
Concept behind alarms	264
Accessing the application.....	264
Defining Alarms.....	265
Alarm Label Definition.....	265
Group Attachments	267
Adding Workstations	268
Viewing the main screen	273
Search	274
Editing.....	275
Exiting Alarm Definitions	276
Tool bar.....	276
Options	276
Notes on associated Transaction Sets	276
Door Forced Open/Door Held Open Alarms.....	277
Old Method	277
New Method.....	279

Alarm Monitor 282

Introduction	282
Alarm information	282
Working with Alarm Monitor	283
Starting the Alarm Monitor.....	283
Active Alarms.....	283
Acknowledged and not secured	284

Pre-defined Alarm Comments.....	284
Acknowledging Alarms.....	284
Viewing and editing Cardholder information	286
Viewing Previous Alarms	287
Executing Override Tasks.....	288
Receiving video of alarms.....	288
Printing the Alarm screen.....	292
Minimize Alarm Monitor	292

Previous Alarms 293

Introduction	293
Accessing the application.....	293
Working with Previous Alarms.....	294
Running a report of Alarms	294
View Alarm Comments	295
Options	295
Tool bar.....	295
Alarm Types.....	296

Alarm State Builder 300

Alarm State Definition	301
Animation Template Definition	302
Animation Script Builder.....	302
Modifying Animation Scripts.....	303
Menu options.....	303
File	304
Search	304
Options	305
Toolbar.....	305
Advance Find	306
Use of Wildcard.....	307

Alarm Graphics-Settings 308

Introduction	308
Navigation View Settings	309
Information Box Setting	311

Alarm Graphics-Editor 312

Introduction	312
Setting up maps and icons	313
Create a New Map	313
Inserting icons on Maps	315
Editing a Map	321

Alarm Graphics-Client 322

Introduction	322
Alarm Notification	323
Alarm Acknowledgement	324
Receiving video of alarms	325
Pre-defined Alarm Comments	329
View Cardholder Image	330
Default State of an Icon	330
Use of Wildcard	331
Advanced Find	331

Transaction Codes Editor 333

Introduction	333
Accessing the application	333
Customizing Transaction Codes	334

Transaction Filters 335

Introduction	335
Accessing the application	335
Defining Filters	335
Creating a Filter Set	335
Creating a Filter	336
Attaching a Transaction to a Filter	336

Editing Filter Definitions	337
Search	337

Transaction Monitor 340

Introduction	340
Accessing the application.....	340
Working with Transaction Monitor	341
Overview	341
Customizing Transaction Codes	341
Selecting a Transaction Group	342
Saving Transaction Monitors	342
Editing Transaction Monitors	343
Pausing Transactions	343
Viewing Cardholder Portrait and Signature.....	344
Playing video file of a Transaction	345
Filtering Transactions.....	345
Pop-up on Transaction.....	346
Options	346
Connecting to Panels via Dial-up	347
Viewing Previous Transactions.....	348
Accessing other applications from Transaction Monitor.....	348

Previous Transactions 349

Introduction	349
Accessing the application.....	349
Working with Previous Transactions	350
Running a Transaction Report.....	350
Printing the screen	350
Tool bar icons	350
Transaction Type Definitions	351
Security Tour System Transactions	353

Manual Overrides 354

Introduction	354
Accessing the application.....	354
Programming Manual Overrides	354
Overview.....	354

Defining Manual Override Sets	354
Defining Manual Override Tasks	355
Defining Manual Override Actions	356
Attaching Tasks to Sets	356
Edit 357	
Executing Override Tasks and Sets	357
Examples of commonly used MRO procedures	357
 Automatic Override Definition	 363

Introduction	363
Accessing the application	363
Working with Automatic Overrides	364
Overview	364
Programming Automatic Overrides	364
Define Automatic Override Tasks	365
Automatic Override Actions	366
Example for an Automatic Override	366
Navigation/Tool bar options	367
Search	367

Universal Triggers	369
---------------------------	------------

Introduction	369
Accessing the application	369
Overview	370
Manual Overrides and Trigger Events	370
Programming a Trigger Event	372
Menu options	373

Elevator Control	375
-------------------------	------------

Introduction	375
Elevator Control Setup	375
Define Areas	376
Define Controllers	377
Define Readers	379
Define Relays	383
Define Contacts	384

Invalid Transactions for Elevator Control	385
Hardware Connection Diagram	386
SIONX 24 wiring Instructions	386

Report Scheduler	389
-------------------------	------------

Introduction	389
Overview	389
Report Scheduler Service	390
Report Scheduler Service Manager	391
Report Scheduler	392
Overview	392
Creating a new Schedule	392
Edit a Schedule	394
Delete a Schedule	394

Report Launcher Settings	395
---------------------------------	------------

Introduction	395
Accessing the application	395
Report Groups and Sub Reports	395
Overview	395
General Settings	395
Creating a new Report Group	396
Creating a new Sub Report	396
Editing and deleting Report Groups	396

Report Launcher	398
------------------------	------------

Introduction	398
Accessing the application	398
Working with Report Launcher	399
Overview	399
Report Groups	400
Base Reports	400
Derived Reports	400
Derived Sub Report (User created)	400
Launching a Report	400
Printing a Exporting Reports	401
Creating a new Sub Report	401

Restoring Archived History	404
Audit Trail-Settings	405
<hr/>	
Introduction	405
Accessing the application	405
Overview	405
Settings	406
Duration of History (in days)	406
Select a Data Table	406
Audit Trail Report	408
<hr/>	
Introduction	408
Accessing the application.....	408
Generating an Audit Trait Report	409
Overview.....	409
End Report.....	409
Understanding a Report.....	410
Rearranging and sorting column titles.....	411
Setting dates	411
CIM	412
<hr/>	
Introduction	412
Settings	412
Creating a CIM Log Directory	412
Starting the CIM	412
Main screen view	413
Options	413
View Settings.....	413
Tool bar icons	414
System Information	415
Status Messages.....	415
Message Logging Priorities.....	415
CIM Start up screen	416
Shutdown/start -up main screen.....	416
Color codes for Com Port Status.....	416
Com Port Expansion	417
COM Port Expansion File Menu.....	417

Definition of fields in the COM Port Expansion window	418
Exiting CIM	419
System Processor	420
Introduction	420
Starting SP	420
Accessing View SP Status	420
Min screen	421
SP Settings	422
Edit options	423
View log file	424
View menu	425
Exiting View SP Status Application	427
Controller Update	428
Introduction	428
Accessing the application	428
Working with Controller Update Utility	429
Overview	429
Reset and Update	429
Information section	430
Communication Status Messages	430
Program Flash	431
Introduction	431
Accessing the application	431
Requirements	432
SRCNX	432
Updating controller memory	432
Notes on upgrading the firmware	433
Offline Lock Interface	434
Introduction	434
Working with Offline Lock Interface	435
Color Schemes	435
Settings	436

Log options	437
Filtering Locks by Areas or Area Set.....	438
Viewing log files	438
Generating programming files.....	439
Error messages.....	439
Closing Offline Lock Interface	439
Working with Uplink.....	440
Accessing the application	440
Uplink configuration	440
Programming	444
Program Locks.....	444
Audit trail.....	447
Date & Time Delays	448
Utilities	449
How to resolve problems with UpLink	450
Working With Schlage Utility Software (SUS)	452
Sync Program Configuration	452
Program Lock	456

Campus Locks 459

Introduction	459
Configuration.....	459
Overview	459
Campus Lock Settings	460
Defining Access Plans for Campus Locks	462
Defining Campus Locks	467
Programming Automatic Overrides for Campus Locks	469
Assigning Access Rights to a Campus Lock	469

CCTV 470

Introduction	470
Accessing the application.....	470
Overview	470
Programming.....	470
Serial Port Communication Test.....	471
Menu Options	472

SVTR 474

Introduction	474
Accessing the application.....	474
Working with SVTR Camera Control.....	474
Configuring Transactions, Devices, Alarms etc.....	475

IR Viewer 478

Introduction	478
System requirements for IR Viewer.....	478
Working with IR Viewer	479
Playback Viewer screen explanation	479
Saving a video clip to a file	480
Save an AVI file	481
Video Compression dialog	481
Saving a MJPEG file	482

Guest Pass Settings 484

Introduction	484
Accessing the application.....	484
Define Settings.....	485
General Setting	485
Access Control.....	486
Defining a Template.....	486
Authorization options	487
Badging.....	488
Label Printing.....	489
Image Verification	490
E-Mail.....	490
Instructions	491
Contacts.....	491
Other	492

Guest Pass Locations	493
Defining a Location	493
Defining a workstation	494
Global Settings	495
Auto Sign-out options	495

Guest Pass System	497
--------------------------	------------

Introduction	497
Overview	497
Color Schemes	498
Creating Guest Records	498
Option 1	498
Adding Portraits to a Badge or a Label	499
Add a Guest	500
Adding Signature to the Badge	505
Authorize a Pending Guest	505
Sign In a Guest	506
Option 2	507
Add, Authorize and Sign In a Guest	507
Option 3	507
Add and Authorize a Guest	507
Sign In a Guest	508
Sign Out a Guest	508
Reset Guests to Pending	509
Editing the Guest Information	510
Description of tabs	511
Delete a Guest Record	511
Search for a Guest	512

On Watch List.....	516
License Field Cross Reference	519
Introduction	519
Accessing the application.....	519
Mapping	519
LockLink Import Wizard	521
Introduction	521
Limitations	522
Imported Data Types.....	523
Importing LockLink Express Database.....	525
Pre-requisites for importing a LockLink Express file	525
Steps for Importing a LockLink Express File.....	525
Importing LockLink 7 Database.....	531
Pre-requisites for importing a LockLink 7 Database.....	531
Steps for importing a LockLink 7 database	532
Warnings and Error Messages.....	536
Schlage GUI Importer	538
Introduction	538
Working with GUI Importer	539
Overview.....	539
Importing text files.....	539
Import Options	540
Linking source columns with Cardholder fields	541
Credential Import Choices	542
Review screen	543
Log file	543
Advanced Importer	545
Introduction	545
Overview	545
Text file format	545
Comment lines	545
Headers	545

Command lines	546
Steps for running the Importer.....	546
Prerequisites	546
Manual execution.....	547
Scheduling for Automatic Import	547
Import Settings	548
Supported commands	549
Commands for adding and deleting cardholders	549
Commands for adding, retiring, and deleting credentials	550
Area Access Commands	552
 Appendix A: MSSQL 2000 Backup and Restore Procedures	557
Backup SQL Database	557
Restore SQL Database	559
 Appendix B: File Space Monitor	563
Introduction	563
Data file utilization in Schlage SMS.....	563
Resolution	564
Step 1	564
Step 2	564
Step 3	564
Step 4 - Backup Database	567
Step 5	567
Schedule Preferences.....	571
Schlage SMS field problems and solutions	573
Scenario 1: - SchlageSQL.NDF too large in size to perform Reindex DB	573
Files and documents included in this package	574
 Appendix C: Database Maintenance Utility	575
Introduction	575
Requirements.....	575
Accessing the application.....	575
Overview	576
Installation and set-up	577
Operation performed by the SQL Agent.....	579
Manual operation of the Database Maintenance Utility	580

Database maintenance procedures for restoring the database	581
--	-----

Appendix D: MSSQL 2005 Server Configuration Settings	585
---	------------

Introduction	585
Settings	585

Appendix E: Schlage SMS Daylight Savings Time Patch	588
--	------------

Glossary of Terms	589
--------------------------	------------

Index	600
--------------	------------

Typographical Conventions

Before you start using this guide, it is important to understand the terms and typographical conventions used in the documentation.

The following kinds of formatting in the text identify special information.

Formatting convention	Type of Information
Numbered (1, 2, 3 ..)	Step-by-step procedures. Users can follow these instructions to complete a specific task.
Bold	Brand names, window names, application name when used for the first time in a chapter or section, items you must select, such as menu options, command buttons, or items in a list.
Notes and warnings	Information that requires special attention of the user.
CAPITALS	Names of keys on the keyboard. for example, SHIFT, CTRL, or ALT.
KEY+KEY	Key combinations for which the user must press and hold down one key and then press another, for example, CTRL+P, or ALT+F4.
<i>Emphasis</i>	Use to emphasize the importance of a point or for variable expressions such as parameters

Acronym

Acronym	Description
CIM	Communication Interface Module
OLI	Offline Interface Module
CL	Campus Locks
CM	Computer Managed
SMS	Security Management System
SP	System Processor
CCTV	Closed Circuit Television
SVTR	Schlage Video Transaction Retrieval System
SRINX	Schlage Reader Interface
SRCNX	Schlage Reader Controller
GUI	Graphical User Interface
UDF	User Defined Fields

Preface

Introduction

The **Schlage Security Management System (SMS)** software offers access control, digital video capture, badging, visitor management, alarm monitoring, security touring and other security applications tailored to every end user. This software manages offline programmable locks, such as Schlage computer-managed (CM) locksets, campus locks, online systems including Schlage value integration package (VIP) and Wireless open architecture locks. Controllers accommodate up to 16 readers, including PIN-enabled locks, magnetic stripe and proximity card readers, iButton readers, and biometric hand readers and finger key readers. An easy-to-use GUI provides “drag and drop” assignment of Areas and Area Sets, Cardholder Categories, Site Codes and Site Code Sets etc.

This user manual provides you guidelines for configuring and customizing the **Schlage SMS** based on your unique company needs. Beginners and experienced users should find the information they need to perform all the administrator and end user activities required to manage the **Schlage SMS**. It also features concise technical discussions, point-by-point guidelines for programming the system, and summaries that give you instant access to the information you need. The end users can also find guidelines for defining cardholders, add credentials, monitoring transactions/alarms, and executing manual overrides.

System Overview

The **Schlage SMS** is a computer based alarm monitoring system that allows cardholders to gain access to a secured area at specific intervals. If a violation occurs the system creates transactions that can be labeled as alarms and sends to appropriate alarm workstations. These secured areas can be controlled from a remote location, from another room or from around the world. The system is also capable of visitor management, advanced reporting, security tour management, badging and digital video recording. The **Schlage SMS** provides offline support for computer managed locks and campus locks. The online system also supports online VIP locks and Wireless readers.

The following sections describe the basics of the system.

Areas, cardholders and readers

An area is a physical space that is used to give access to a cardholder, which represents a person who is interacting with the **Schlage SMS**. A cardholder swipes a credential, or enters a pin number at the reader or keypad. An area can have one or more readers attached to it. For example a main lobby in a building with four entrances can have four readers but it can be defined as one area called “Main Lobby”. That way a cardholder can gain access through these four doors by having access to one single area. The area record is downloaded to the controller only once and that saves the memory on the controller. It is important to note that a reader must be associated with only one area, although an area can have multiple readers associated with it.

Grouping Structure - Area Sets and Cardholder Categories

The areas and cardholders can be grouped as sets and categories to grant access easily. For example, a user can create a cardholder category called “IT Department” and include all the IT employees in that category. The user can also create an area set called “IT General” including all the IT areas.

Area Access

Cardholders are given access to areas during a specific timezone. Some other specific details about the access include door type (disabled access, pedestrian access etc.) and area state (this allows the software to deal with strike, lock down etc.). The door types and area states are user definable.

Credentials

Cardholders can own zero or more Credentials. A credential is a physical or logical object used at a reader to prove one's identity; common credentials are badges, iButtons, proximity key fobs, PINs, etc. Credentials are not involved in granting access; they are simply used to establish who someone is. Consequently, if a cardholder has more than one credential, he can use any of them to enter an area he has been given access to, provided a reader that can physically read that credential is available.

Transactions

Transactions are the events that happen in the **Schlage SMS**. "Valid Access", Access Denied" Relay Energized" etc. are some examples of transactions that can occur in the security management system. Every transaction is associated with a time, type and other information associated with it depending on the type of the transaction. Transactions are used for alarming, reporting and monitoring.

Online and Offline Access Control

The **Schlage SMS** supports both online and offline access control. In the online system a read head is connected to a reader interface which is in turn connected to a reader controller.

Read heads are the transducers that actually interact with a credential; for instance a slot through which a magnetic stripe is swiped, or a keypad into which a pin number is entered. Reader interfaces are pieces of hardware that decode the data encoded on the credential into a set of numbers usable by the controller. Controllers store information about cardholders and access and implement the access control logic (the controller decides whether the door should open in response to a credential). Controllers remain in constant communication with the software.

Offline locks are standalone locks with a credential reader that are installed in a door, on a door frame, or near a door and are not connected to an external online controller. They are programmed and audited using a PDA or similar device.

Communication

These are the main entities involved in the system communication.

- **SQL Server** - SQL Server is a database system where all information associated with the security system is stored.
- **SP (System Processor)** - The SP is the communication hub in **Schlage SMS**. There is only one instance of the SP running in a system, no matter how large the system is. It is commonly run on the same physical machine as the SQL Server.
- **CIM (Communication Interface Module)** - The CIM is a client application responsible for handling the communication to the controllers in the field. Many systems have only one CIM, running on the same physical machine as the SQL Server, but larger systems can have several or even dozens of CIMs.
- **Controllers** - Controllers are pieces of hardware that have devices such as relays, contacts and card reader interfaces connected to them. These controllers make the decisions about whether to grant access to cardholders when they present a credential to a card reader. They also monitor contact points, energize relays based on schedules, etc. Controllers are also commonly referred to as panels or SRCNXs.

Communication between CIM and controllers

The following section gives you an overview of online communication in Schlage SMS.

A CIM can be connected to many controllers at once. Communication occurs via the network, a COM port, or a dial-up modem. The CIM downloads information about badges, schedules, etc. to controllers; occasionally downloads new firmware to controllers and collects transaction information from the controllers. A list of both connected and disconnected controllers can be viewed at the CIM.

The controller is responsible for initiating the connection to the CIM; the CIM does not actively attempt to connect to controllers. Networked controllers will attempt to connect to the CIM at whatever IP Address was programmed into them during setup. This programming of the controller's network device is commonly done via telnet, a web interface, or the Lantronix Device Installer application.

CIM to SP communication

The CIM connects to the SP upon startup and sends transactions to it as soon as they are gathered from controllers. If the CIM cannot connect to the SP, it will stop accepting transaction information from the controllers, causing them to be buffered there until the CIM can connect to the SP. This is to prevent a transaction that could potentially generate an alarm from bypassing the SP.

CIM to database communication

The CIM communicates to SQL server like any other client application. It writes transactions to the database as they are gathered from controllers. If the CIM cannot connect to the database, it will stop accepting transaction information from the controllers, causing them to be buffered there until the CIM can connect to the database. This is to prevent these transactions from being lost should the CIM be stopped before database communication is reestablished.

CIM to workstation communication

The CIM listens on port 5354 for connections from other Schlage SMS client applications. The primary usages of this communication are to allow other workstations to issue Manual Overrides (for instance, opening a door) and to allow other workstations to flash new firmware into the controllers.

Controller behavior when offline

When the controller is not connected to the CIM, it continues to function normally using the last information sent to it. This is to ensure people can continue to open doors regardless of the state of the CIM. It will buffer as much transactional information as it can until it runs out of memory, waiting for the CIM to come back online. Once memory is full, it will overwrite the oldest transactions in the buffer with new transactions. This storage capacity depends on how much memory is installed in the controller as well as how rapidly transactions are being generated.

Transactions and Alarms

Transactions are received from the SRCNX panels at the CIM. Once the CIM receives the transaction, the CIM writes this transaction to the SQL database located on the server and then receives an acknowledgement back from the database. The CIM then passes the transaction to the SP. The SP then determines if this transaction is an alarm. This procedure is accomplished by the SP reviewing the alarm labels and attachments. If the transaction is determined as an alarm, it is written to the SQL database. Then the SP receives an acknowledgement back from the SQL database. Then the SP sends this alarm to the appropriate alarm workstation. Once the transaction is properly handled (acknowledged), the details pertaining to the transaction are written to the SQL database.

Schlage SMS Levels

The **Schlage SMS** software is available in multiple levels to fit your current needs and budget. Users can seamlessly migrate to new levels as their security requirements change while leaving existing databases, PCs and hardware intact. The following are the three software levels:

- **Schlage SMS Select**
- **Schlage SMS Premier**
- **Schlage SMS Enterprise**

Levels and available modules

Note: The levels do not apply outside of North America.

Features/Modules	Select	Premier	Enterprise
System Settings	Yes	Yes	Yes
System Security	Yes	Yes	Yes
CIM		Yes	Yes
SP		Yes	Yes
CM Offline Lock Management	Yes	Yes	Yes
CL Offline Lock Management	Yes	Yes	Yes
Online credential definition and area access assignment		Yes	Yes
Card Format Editor		Yes	Yes
Database Maintenance Utility	Yes	Yes	Yes
Badging	Yes	Yes	Yes
Transaction Monitoring		Yes	Yes
Transaction Codes Editor		Yes	Yes
Previous Transactions		Yes	Yes
SVTR		Yes	Yes
Alarm Monitor		Yes	Yes
Alarm Graphics		Yes	Yes
Portrait Monitoring		Yes	Yes
Reports	Yes	Yes	Yes
Audit Trail Report			Yes
Audit Trail Control			Yes
History Archive		Yes	Yes

Features/Modules	Select	Premier	Enterprise
Manual Overrides		Yes	Yes
Automatic Overrides		Yes	Yes
Universal Triggers		Yes	Yes
Controller Update Utility		Yes	Yes
Guest Pass System		Optional	Yes
SEVMS		Yes	Yes
LL Importer	Yes	Yes	Yes
File Space Utility	Yes	Yes	Yes
Schlage GUI Importer	Yes	Yes	Yes
Email Editor			Yes
Team Definition			Yes
Alarm Graphics		Yes	Yes

Installation and Getting Started

CHAPTER 1

Introduction

This section gives you instructions for installing the software, user login and details about **System Launcher** (on page 42). The steps in the installation may slightly vary depending on the level of software you are installing.

Operator's requirements

- 1 You must be the owner of Schlage SQL database.
- 2 You must have administrator rights to the PC and the Schlage SMS folder.

If you meet all the requirements mentioned above, you can proceed with the **Schlage SMS** installation program.

Note: While installing the SQL Server, make sure that the case sensitivity option is turned off. If this SQL setting is turned on, **Schlage SMS** installation will fail.

Minimum PC requirements

- 1 Pentium III 700 MHz with 512 MB RAM (preferably 1GB) and 40 GB Hard drive.
- 2 Operating System:
 - Single User - Windows XP Professional/ Windows 2000 Professional/Windows Vista/Windows 7
 - Multi User - Windows 2000 Server/ Windows 2003 Advanced Server/ Windows 2008 Server
- 3 Database Engine:
 - Single User - MSDE 2000 SP4/MS SQL Server 2000 Desktop Edition SP 4, MS SQL Server 2005 SP 1
 - Multi User - MS SQL Server 2000 SP4, MS SQL Server 2005 SP 1
- 4 MDAC 2.8 SP1

Tip: A free version of this software can be downloaded from www.microsoft.com/downloads/search.asp

Note for McAfee Virus Protection users: Prior to the software installation, completely close the antivirus application. McAfee should also be closed after each reboot during installation process if virus protection is set as an auto-start when operating system starts. McAfee is known to interfere with **Schlage SMS** modules, especially Cardholder Definition, because it considers them to be "computer viruses". At this time, we are not aware of any other virus protection application that is not compatible with **Schlage SMS**. Symantec Antivirus is compatible and the recommended virus software to use with **Schlage SMS**.

Installation instructions

SQL Server Version verification

- 1 The first step in the installation process is determining the version of the SQL Server. **Schlage SMS** does not support systems with MS SQL Server 7 and MSDE 7. If the installation/upgrade detects MS SQL Server 7 on the PC where you are installing Schlage SMS, the installation process will abort. Please contact technical support (866-322-1237) for further assistance. If the upgrade detects MSDE 7 installed on the PC, the user has an option to upgrade the database engine from MSDE 7 to MSDE 2000.

Enter the password for the database login in the following window, and **Next** to continue.



Note: Schlage SMS supports Microsoft SQL Server 2005 Standard and Enterprise editions.

Server Install (10 users or more)

Note: Five (5) users or less go to the 'Server Install (5 Users or less)' section.

- 1 Insert the CD labeled **DB Engine Installation**. The Wise installation program begins automatically. Select **Install the DB Engine**.

Note: If Windows XP SP 1, Internet Explorer 5.5 or higher, MSDE 2000 with SP 4 are already installed on your machine, you can skip steps 2 - 5 and go to step 6.

- 2 Installation of **Windows Service Packs**.

- a) Windows 2000 - If Service Pack version is less than 4, you will be notified that there is a service pack available.
- b) Windows XP - If Service Pack version is less than 2, you will be notified that there is a service pack available.

Note: If Windows 2000 SP4/Windows XP SP2 or higher is already installed on your machine, you can skip this step.

- 3 Internet Explorer 5.5 or higher must be installed. If not, you will be prompted to install it. Once the Internet Explorer is installed, restart this installation.

Note: If Internet Explorer 5.5 or higher is already installed on your machine, you can skip this step.

- 4 MS SQL Server 2000 or MS SQL Server 2005 must be installed on your machine. If not, SQL 2005 will be installed.

Note: If MS SQL Server 2000 or MS SQL Server 2005 is already installed on your machine, you can skip this step. When utilizing MS SQL Server 2000, a licensing agreement must be obtained from Ingersoll-Rand Security Technologies prior to this installation.

- a) The **Database Engine License Agreement** window opens. After reading the License Agreement, Select *I Agree* and click **Next** to continue, or select *I Disagree* and click **Cancel** to abort the installation.
 - b) Database Engine installation begins. This process may take 5 -10 minutes. Once the Database Engine window opens, click **OK** and restart your machine. The software installation will restart automatically.
- 5 If the machine has MS SQL Server 2000 installed, the SP 4 must be installed on your machine. If not, you will be prompted to install it. Remember that it is required for the proper functionality of the software. Click **Yes** to start the installation.
- a) The **Welcome** window opens, click **Next**.
 - b) The **Software License Agreement** window opens. After reading the License Agreement, click **Yes** to continue the installation or click **No** to abort the installation.
 - c) The **Instance Name** window opens. Click **Next**.
 - d) The **SQL Server 2000 Service Pack 4 Setup** window opens. Select *Upgrade Microsoft Search and apply SQL Server 2000 SP4*. Click **Continue**.
 - e) The **Error Reporting** window opens, click **OK**.
 - f) The **Start Copying Files** window opens. Click **Next**.
 - g) The **Setup Complete** window opens. Click **Finish** and restart your machine.
 - h) After you restart your machine insert the CD labeled Software Installation. The installation program begins automatically. Select **Install the Software - Server**.

Server Install (5 users or less)

Note: If Windows 2000 SP 4/Windows XP SP 2, IE 5.5 or higher, MSDE 2000 with SP 4 are already installed on your machine, you can skip steps 7 - 9 and go to step 10.

- 1 Installation of Windows Service Packs
 - a) Windows 2000 - If Service Pack version is less than 4, you will be notified that there is a service pack available.
 - b) Windows XP - If Service Pack version is less than 2, you will be notified that there is a service pack available.

Note: If Windows 2000 SP4/Windows XP SP2 or higher is already installed on your machine, you can skip this step.

- 2 **Internet Explorer 5.5** or higher must be installed. If not, you will be prompted to install it. Once the **Internet Explorer** is installed restart this installation.

Note: If Internet Explorer 5.5 or higher is already installed on your machine, you can skip this step.

- 3 MSDE 2000 with SP4 must be already installed on your machine. If not, it will be installed.

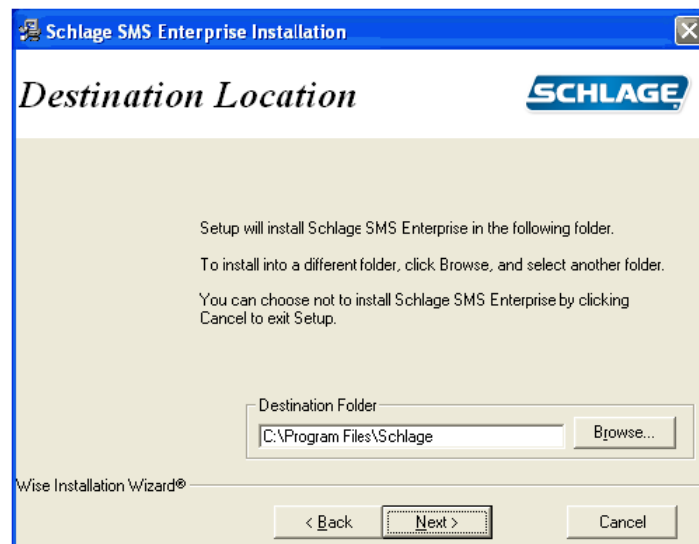
Note: If MSDE 2000 is already installed on your machine, you can skip this step.

- a) Database Engine installation begins. This process may take 5 -10 minutes.

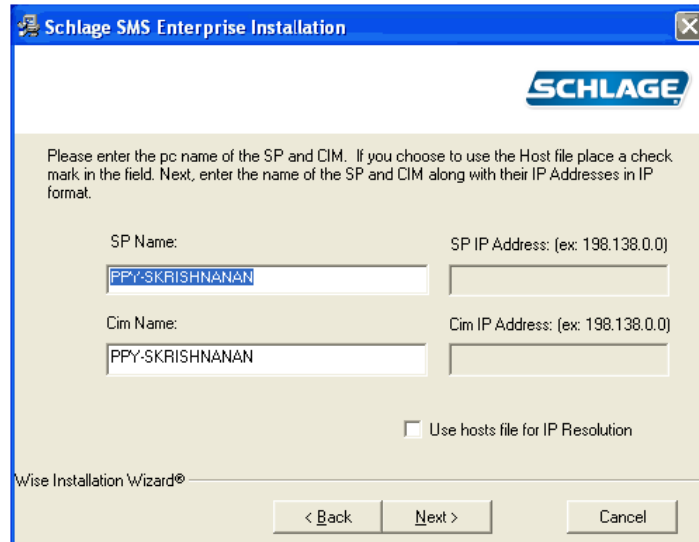
- b) Once the installation completes you will be prompted to restart your pc. Click **Yes**, the Schlage software installation will restart automatically.
- 4 MDAC 2.8 SP1 must be already installed on your machine. If not, you will be prompted to install it. Click **OK** to begin the installation.
 - a) The End User License Agreement window opens. Read the License Agreement carefully before proceeding with the installation of the software. Select *I Accept all of the terms of the preceding license agreement* and click **Next** to continue, or click **Cancel** to abort the installation.
 - b) The **Installing the Software** window opens. Click **Finish** to begin the installation.
 - c) MDAC 2.8 SP1 installation begins. This process may take 5 -10 minutes.
 - d) The **Restarting the System** window opens. Select **Let setup restart the system now** and click **Finish**. The installation will restart automatically.

Schlage SMS Software Installation

- 1 The **Schlage SMS** software Installation starts. The **Welcome** window opens. Click **Next**.
- 2 The **License Agreement** window opens. Read the license agreement carefully before the installation of the software. Select *I Agree* and click **Next** to continue, or select *I Disagree* and click **Cancel** to abort the installation.
- 3 The **Destination Location** window opens. Click **Next** to accept the default location or click **Browse** to choose a different destination.

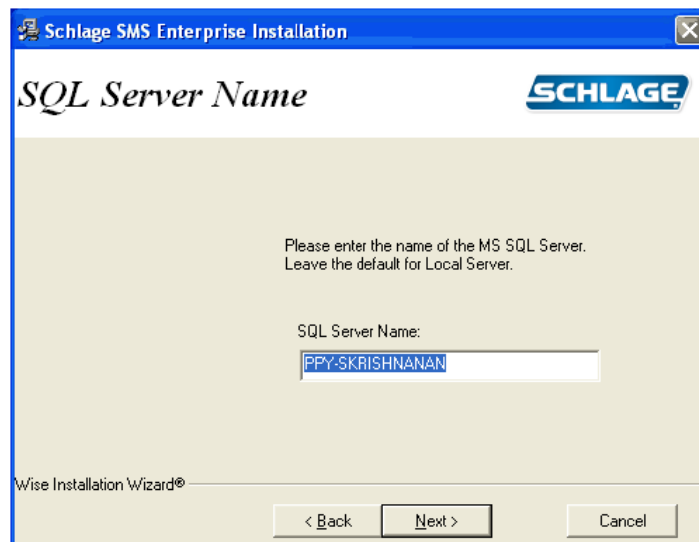


- 4 The **Client/Server Setup** window opens.



The screenshot shows the 'Schlage SMS Enterprise Installation' window. The title bar is blue with the Schlage logo. The main area has a light beige background. At the top, there is a blue bar with the Schlage logo. Below it, a text box says: 'Please enter the pc name of the SP and CIM. If you choose to use the Host file place a check mark in the field. Next, enter the name of the SP and CIM along with their IP Addresses in IP format.' There are four input fields: 'SP Name:' with 'PPY-SKRISHNANAN', 'SP IP Address: (ex: 198.138.0.0)', 'Cim Name:' with 'PPY-SKRISHNANAN', and 'Cim IP Address: (ex: 198.138.0.0)'. There is a checkbox labeled 'Use hosts file for IP Resolution' which is currently unchecked. At the bottom, there is a 'Wise Installation Wizard®' logo and three buttons: '< Back', 'Next >', and 'Cancel'.

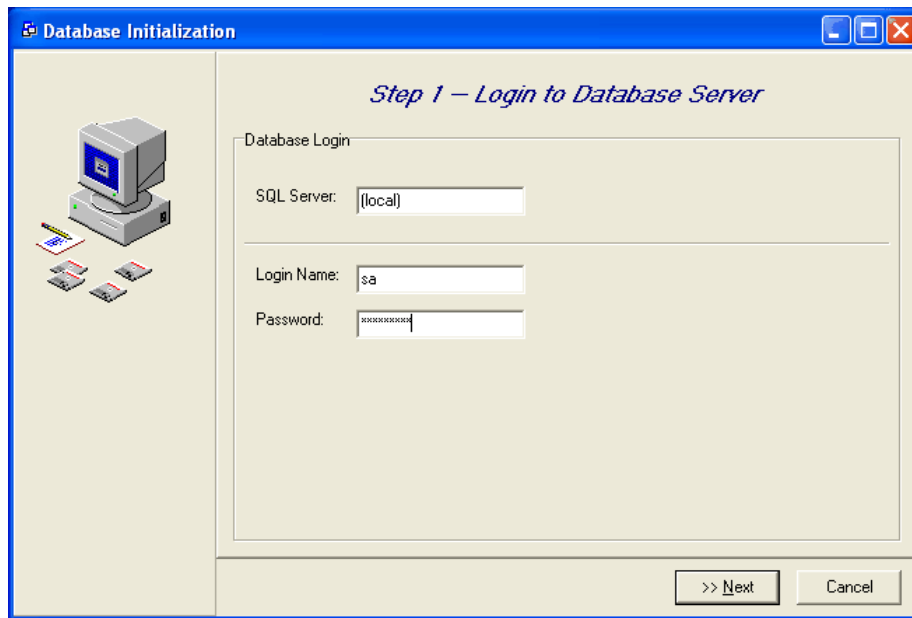
- a) Enter the NetBios/machine name where the SP and CIM applications will reside. For Single User systems leave the default values.
- b) You can also enable the **Use hosts file for IP Resolution** check box to modify and change the name to your preference and use the IP address of the machine where the SP and CIM applications will reside. Click **Next**.
- 5 The **SQL Server Name** window opens.



The screenshot shows the 'Schlage SMS Enterprise Installation' window with the title 'SQL Server Name'. The title bar is blue with the Schlage logo. The main area has a light beige background. At the top, there is a blue bar with the Schlage logo. Below it, a text box says: 'Please enter the name of the MS SQL Server. Leave the default for Local Server.' There is one input field labeled 'SQL Server Name:' with 'PPY-SKRISHNANAN'. At the bottom, there is a 'Wise Installation Wizard®' logo and three buttons: '< Back', 'Next >', and 'Cancel'.

Note: Before proceeding with the installation, verify how the Microsoft SQL Server is installed. When the SQL Server is installed, if the default computer name was used, you can accept the default value (local). If an instance of the SQL Server is used you must enter the full path name and the name of the instance. Example: \\COMPUTER-146\\INSTANCE NAME. If you face any problems during the process (finding out how the SQL Server is installed) please consult with your IT department. If the SQL Server name is incorrect, the installation will fail.

- 6 The **Schlage SMS** software installation continues. The **Database Initialization** window opens.
- a) The **Step1 - Login to Database Server** window opens. Enter the password for the 'sa' login. If the SQL Server/MSDE was installed using our wise installation, enter "SECAdmin1" as the password. Click **Next**.



Note: Very Important: Before proceeding with the installation, verify how the Microsoft SQL Server is installed. When the SQL Server is installed, if the default computer name was used you can accept the default value (local). If an instance of the SQL Server is used you must enter the full path name and the name of the instance. Example: \\COMPUTER-146\\INSTANCE NAME

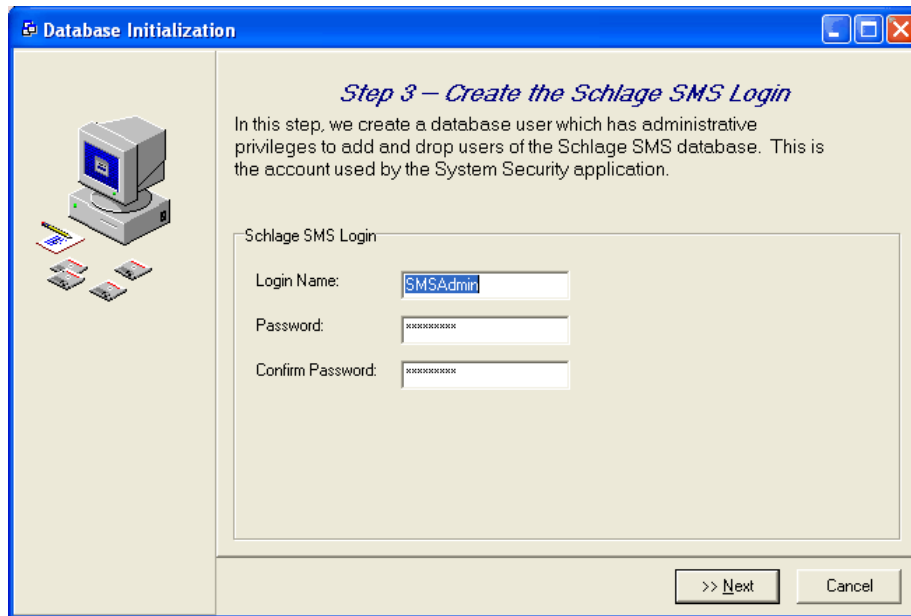
If you face any problems during the process (finding out how the SQL Server is installed) please consult with your IT department. If the SQL Server name is incorrect, the installation will fail.

- b) If you are installing this software on a system that previously had **Schlage SMS** software, the **Database Already Exists** window opens. Read the message carefully and make your decision.
-

Note: Be extremely careful in making a decision here. If your system is already running **Schlage SMS** software and you continue with the installation of the software, you run the risk of losing the existing data on your database. So it is very important to decide whether you want to install the software again.

- c) The **Step 2 - Create Schlage SMS Database** window opens displaying the paths of different database folders. If the paths are correct, click **Next**. Otherwise, click **Set File Paths** and select the path for the different folder and click **OK**.

- d) The **Step 3 - Create the Schlage SMS Login** window opens. Keep the default values (SMSAdmin, SECAAdmin1) and click **Next**.



- e) The database initialization starts displaying the scripts as they are run.
- f) The **Database Initialization Complete** window opens click **OK**.
- 7 The **Schlage SMS** software installation continues. The **Database Initialization** window opens. Follow steps (a) through (f) above to initialize the template database.
- 8 If you chose **Yes** on the previous screen, the **Sentinel Protection Installer-Installation Wizard** is displayed. Click **Next**. Accept the default values throughout the installation.
- a) The **Program Maintenance** window opens. Choose the function you want to perform. The choices are:
- Modify** - This option allows you to select the features that are installed.
 - Repair** - This option allows you to correct any errors that occur while installation.
 - Remove** - This option removes the **Sentinel Protection Installer** from your PC.
- Select one of the above options by clicking on the radio button, and click **Next**.
- b) The **Setup Type** window opens. Select Complete and click Next.
- c) The **Ready to Install the Program** window opens. Click Install.

Note: Remove all USB keys before continuing.

- d) If Windows XP/2003 is installed a window will come up asking to modify the firewall settings. Click **Yes**.
- e) The **Installation Completed** window opens. Click **Finish**.
- f) The **Finished!** window opens. Click **Finish**.

Client Installation/Upgrade

- 1 Insert the CD labeled **Software Installation**. The installation program begins automatically. Select **Install the Software - Client**.
- 2 Installation of **Windows Service Packs**.
 - a) Windows 2000 - If Service Pack version is less than 4, you will be notified that there is a service pack available.
 - b) Windows XP - If Service Pack version is less than 2, you will be notified that there is a service pack available.

Note: If Windows 2000 SP4/Windows XP SP2 or higher is already installed on your machine, you can skip this step.

- 3 The **Welcome** window opens. Click **Next**.
- 4 If you already have the client software installed on your machine and are upgrading to the latest version the **Ready to Upgrade** window opens. Click on **Next** to start the upgrade and skip steps 5 to 9.
- 5 The **License Agreement** window opens. Read the License Agreement carefully before the installation of the software. Select *I Agree* and click **Next** to continue, or select *I Disagree* and click **Cancel** to abort the installation.

Note: This window will not show up if the wise detects a previous installation on your machine.

- 6 The **Destination Location** window opens. Click **Next** to accept the default location or click **Browse** to choose a different destination.

Note: This window will not be displayed if the installation program detects a previous installation on your machine.

- 7 The **Location on Server** window opens, browse to the Schlage directory located at the Server. Click **Next**.

Note: This window will not be displayed if the wise detects a previous installation on your machine.

- 8 The **Client/Server Setup** window opens.

Note: This window will not show up if the wise detects a previous installation on your machine.

- a) Enter the NetBios/machine name where the SP and CIM applications will reside.

You can also enable the Enable host file for IP Resolution check box to modify and change the name to your preference and use the IP address of the machine where the SP and CIM applications will reside. Click **Next**.

- 9 The **SQL Server Name** window opens. Enter the name of the SQL Server machine. Click **Next**.

Note: Before proceeding with the installation, verify how the Microsoft SQL Server is installed. When the SQL Server is installed, if the default computer name was used you can accept the default value (local). If an instance of the SQL Server is used you must enter the full path name and the name of the instance. Example: \\COMPUTER-146\\INSTANCE NAME. If you face any problems during the process (finding out how the SQL Server is installed) please consult with your IT department. If the SQL Server name is incorrect, the installation will fail.

The MSSQL Server window will not be displayed if the wise detects a previous installation on your machine.

- 10 The installation process continues. The **Client Settings** window is displayed. If the default password for the 'SMSAdmin' login was changed during the server installation, please enter the new password. Otherwise leave the default values, and click **Next**.

- 11 The **Software Key Settings** window opens. Click **Yes** if this is the machine where the SP will reside, otherwise click **No**.
- 12 If you chose **Yes** on the previous screen, the **Sentinel Protection Installer-Installation Wizard** is displayed. Click **Next**. Accept the default values throughout the installation.
 - a) The **License Agreement** window opens. Select *I accept the terms in the license agreement* and click **Next**.
 - b) The **Setup Type** window opens. Select **Complete** and click **Next**.
 - c) The **Ready to Install the Program** window opens. Click **Install**.

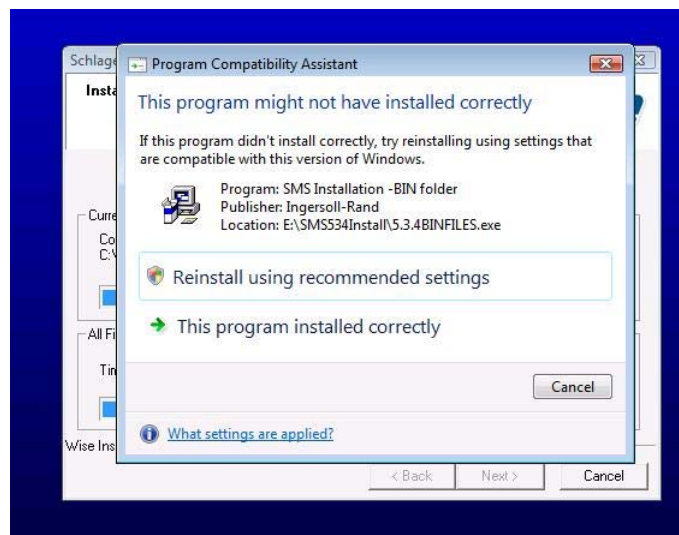
Note: Remove all USB keys before continuing.

- 13 If Windows XP/2003 is installed you will be prompted to modify the firewall settings. Click **Yes**.
- 14 The **Installation Completed** window opens. Click **Finish**.
- 15 The **Finished!** window opens. Click **Finish**.

Notes on Windows Vista/Windows 7 Install

Program might not have installed correctly

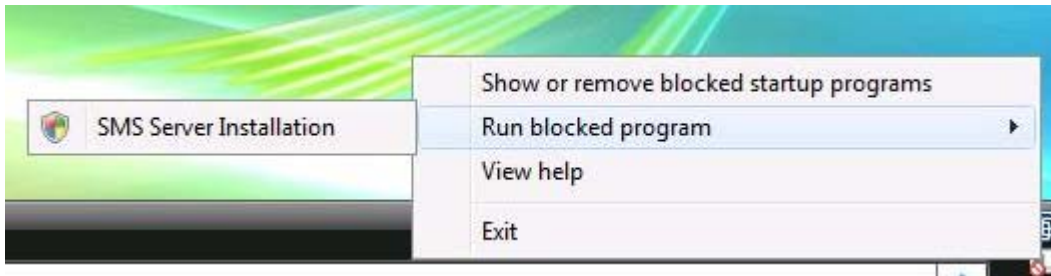
During the installation of SMS on Windows Vista or Windows 7, when the WISE Installer invokes the **5.3.4BINFILES.EXE**, **DBINSTALL**, and **54_Arc~1** a message will pop up stating that: "This Program might not have installed correctly"



Click on the **This Program has installed correctly** option and SMS will continue installing. Do this any time this message comes up.

Blocked Programs

When installing SMS in Windows Vista or Windows 7, upon the first reboot after the database engine has been installed, you will get a message stating that Vista blocked some programs from starting.



Click on the Run blocked program option and SMS will start correctly.

Upgrade instructions

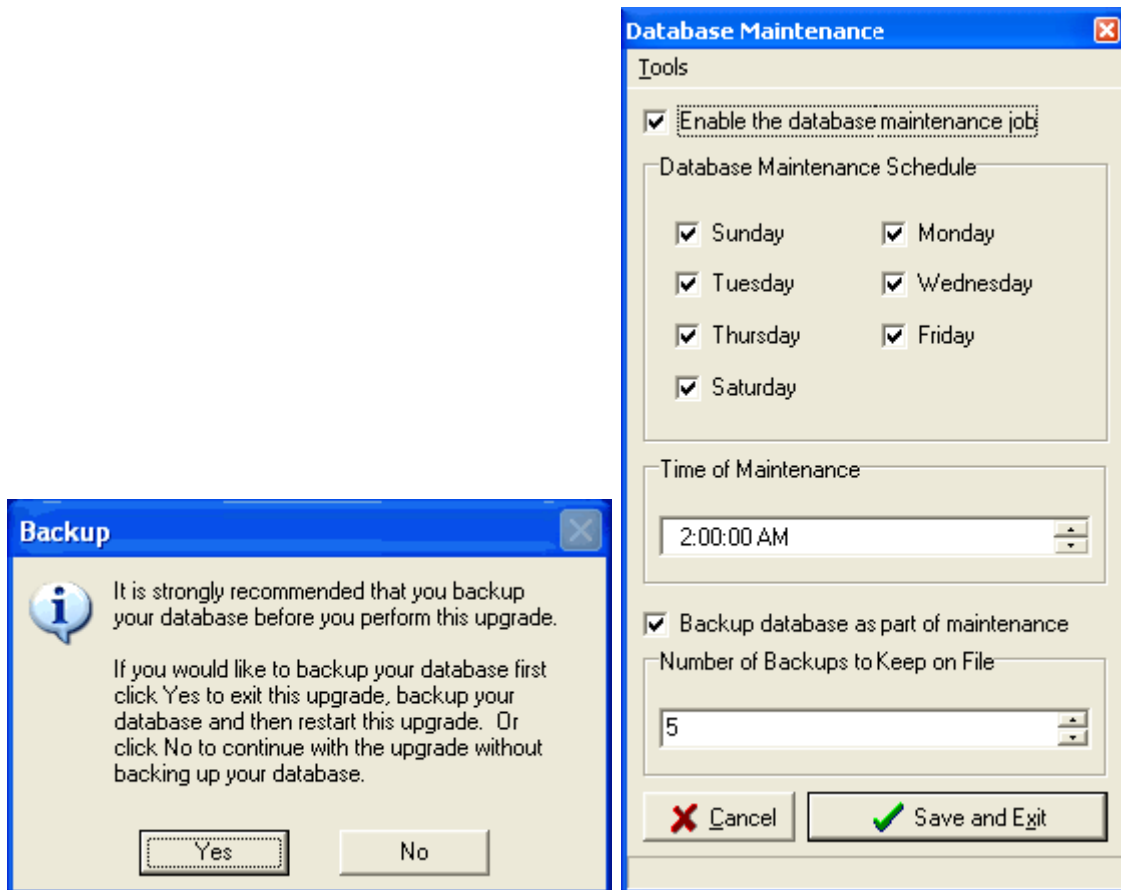
Note: Geoffrey Access Control Systems can only be upgraded to Schlage SMS Enterprise.

Server Upgrade

Note: Prior to performing the upgrade, discuss the backup procedures with your IT department.

In order to run the upgrade, the operator must be the owner of SchlageSQL database. Also, the operator must have administrator rights to the PC and the **Schlage SMS** folder where the **Schlage SMS** is installed.

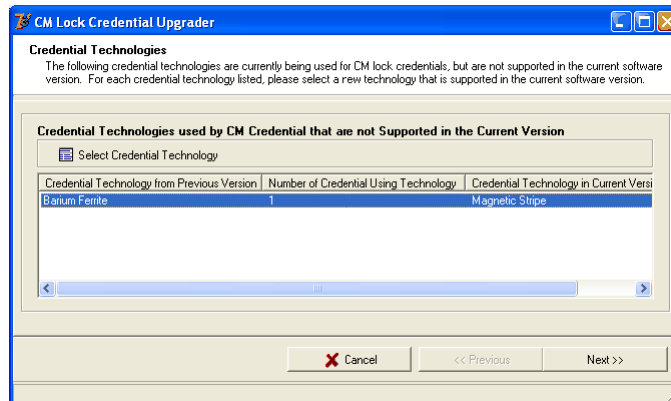
- 1 Insert the enclosed CD-ROM. The upgrade begins automatically. Select **Run the Upgrade**. The first step is determining the SQL Server version. Schlage SMS does not support systems with MS SQL Server 7 and MSDE 7. If the installation/upgrade detects MS SQL Server 7 on the PC where you are installing **Schlage SMS**, the installation process will abort. Please contact technical support (866-322-1237) for further assistance. If the upgrade detects MSDE 7 installed on the PC, the user has an option to upgrade the database engine from MSDE 7 to MSDE 2000. Enter the password for the database login in the following window, and **Next** to continue.
- 2 The upgrade needs a certain amount of free disk space on the same volume where the log file resides. Wise installation performs this check and if there is not enough space a warning message is displayed. If you continue with the upgrade it is strongly recommended that you backup the database. If you would like to do a backup, click **Yes** to exit, backup your database, and then restart this upgrade or click **No** to continue without backing up your database (if the upgrade fails you will not be able to recover your database). If there is enough space the **Login** window opens. Enter your database login and password.



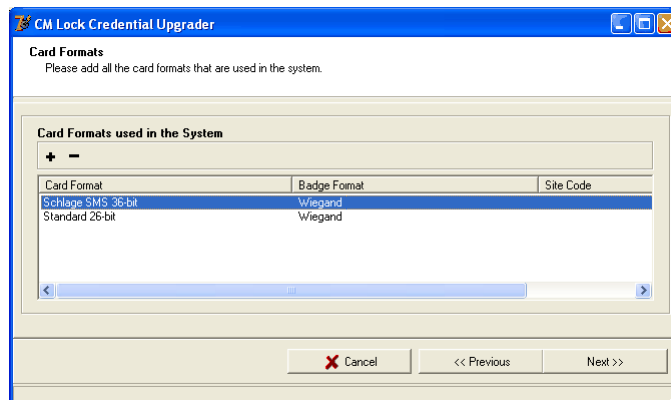
- 3 MDAC 2.8 SP1 must be already installed on your machine. If not, you will be prompted to install it. Click **OK** to begin the installation.
 - a) The **End User License Agreement** window opens. Read the License Agreement carefully before the installation of the software. Select **I Accept** all of the terms of the preceding license agreement and click **Next** to continue, or click **Cancel** to abort the installation.
 - b) The **Installing the Software** window opens. Click **Finish** to begin the installation.
 - c) MDAC 2.8 SP1 installation begins. This process may take 5 -10 minutes.
 - d) The **Setup is Complete** window opens. Click **Close** to exit MDAC installation.
- 4 The **Welcome** window opens. Click **Next**. Notice that the **Back** button is disabled on the **Welcome** screen. Once you are on the **Welcome** screen, and if you still want to back up the database, the **Database Maintenance Utility** (DatabaseMaintenance.exe) is accessible from the Bin directory. (Users do not need to exit the Wise Installation program in order to perform a backup.) If an error occurs during the upgrade, and no backup is available, all the data in the database may be lost.
- 5 The **Ready to Upgrade** window opens. Click **Next**.
- 6 The **Database Upgrade Utility** window opens. Click **Next**.

Note: Various housekeeping messages are displayed on your screen. Depending on the size of your database this upgrade will take some time.

- 7 Next, the **CM Lock Credential Upgrader** window is displayed. The utility must be run on all version 5.1.3 and version 5.1.4 systems that have active CM lock credentials. It first identifies credentials that use unsupported technologies like Barium Ferrite and replaces such technologies with the supported technologies like Proximity or Magstripe. The example below lists one credential that uses Barium Ferrite as credential technology. Highlight the record and click on the **Select Credential Technology** button located on top of the window. Notice that the Next button is enabled now; it is disabled until you select a replacement technology. Click **Next**.



Also, in order to upgrade a credential, the utility needs to know its format. Next step is to select the Card Formats Used in the System. Click on the + (add) button, and the Search window displays the available card formats. Highlight a record and click **OK**. The utility upgrades only the credentials that are in the selected card formats. If a card format is missing from the list, all credentials in that format will not be upgraded. Click **Next** to proceed.



The utility displays a list of credentials that need to be upgraded and continues with the upgrade process. The Save button on the top right corner allows users to save the list of credentials that will be updated in html file. Once the process is completed, click **Finished** button to exit the program and continue with wise installation.

- 8 Once the upgrade is done click **Finish**. If you have CCTV, Guest Pass System or Report Scheduler installed on your machine the wise installation will automatically upgrade them.
- 9 The **Software Key Settings** window opens. Click Yes if this is the machine where the SP will reside, otherwise click **No**.
- 10 If you chose **Yes** on the previous screen, the **Sentinel Protection Installer 7.3.0** window comes up. Click **Next**. Accept the default values throughout the installation.

- 11 The **License Agreement** window opens. Select *I accept the terms in the license agreement* and click **Next**.
 - a) The **Setup Type** window opens. Select Complete and click **Next**.
 - b) The **Ready to Install the Program** window opens. Click **Install**.

Note: Remove all USB keys before continuing.

- c) If Windows XP/2003 is installed a window will come up asking to modify the firewall settings. Click **Yes**.
- 12 The **Installation Completed** window opens. Click **Finish**.
- 13 The **Finished!** window opens. Click **Finish**. Once the software is successfully upgraded, the Database Maintenance Utility is launched to recreate the purge procedures.

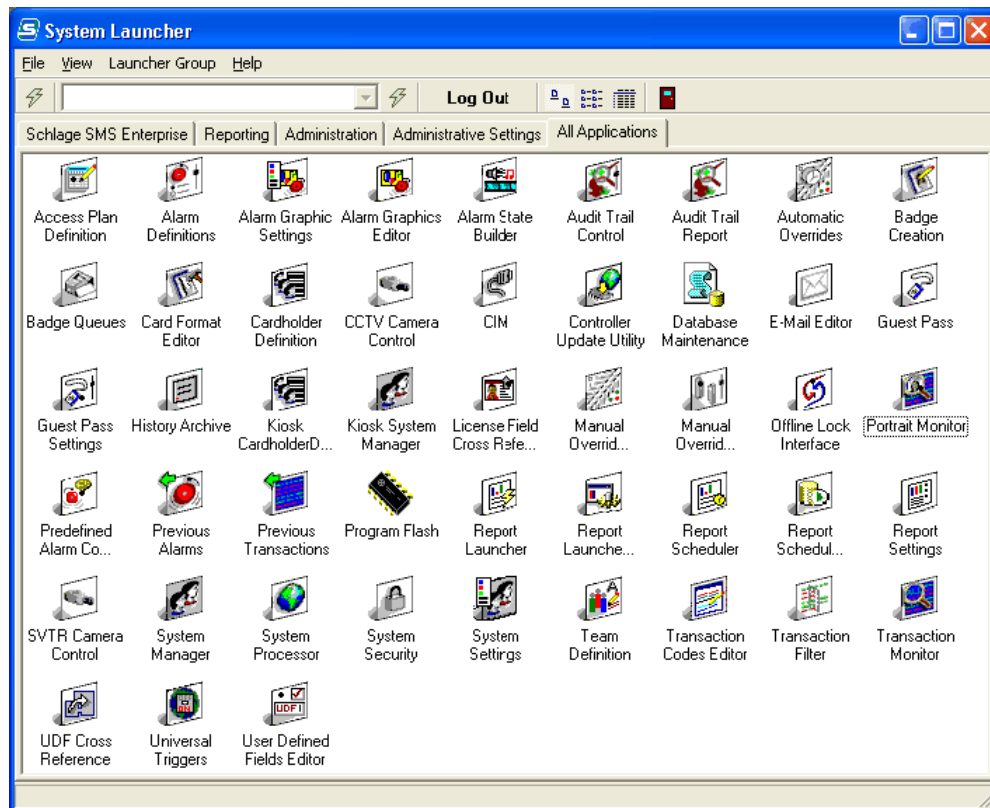
Guest Pass System Installation (only applicable to Schlage SMS Premier users)

- 1 Insert the CD ROM. The **Guest Pass System for V5.3.5 Main Menu** is displayed.
- 2 Select the option **Install Software**.
- 3 The wise installation begins. This installation is only compatible with **Schlage SMS Premier**. If the installation process detects a different version of the software, the installation will exit.
- 4 The **Welcome** window opens. Click **Next** to start the installation. Use **Back** to go the previous step and **Cancel** to abort the program.
- 5 In the next window click **Next** to install **Guest Pass System** application. It takes only a few seconds to finish the installation. Click **Finish**.
- 6 If you are using the **Scan Shell 800 driver's license scanner**, connect the scanner to the workstation.
- 7 In **New Hardware Wizard**, they have to use the option to **SELECT A LOCATION** for the driver files and browse to the Scanshell folder on the CD.

System Launcher

The user can access the **Schlage SMS** modules using the launcher. The system launcher program can be customized by creating launcher groups. The modules available for a user are based on the user login. The icons representing the applications can also be re-arranged separately for each group.

Note: The version of the database must match with the version of the System Launcher. If there is a mismatch between these two, the System Launcher cannot be run.



Note: System Launcher is two separate programs, LauncherV5.exe and LauncherGUI.exe. This is not visible to a user except as a process in Windows Task Manager.

Creating Launcher Groups

- 1 Select **Launcher Group>New Group**.
- 2 In the **New Group** window, enter a name for the group and click **OK**. The new group tab appears on the launcher window next to the all applications tab.

Default user ID and password

Schlage Software is shipped with default User ID and Password given below:

User ID = USR

Password = password

Note: Password is case sensitive. Use lower case letters while typing password. Otherwise you may get an Access Denied message.

- 1 From the desktop click on **System Launcher** icon.



- 2 Enter your assigned user id and the password. The system launcher window is displayed.

Note: The modules that are available on this screen depend on the security group you are assigned to and the privileges that group has. See System Security chapter for further details.

Adding applications to the Launcher Group

Note: The applications in the **All Applications** factory set tab cannot be modified. This tab always has all applications the current user has permissions to launch.

- 1 To add applications to user created groups, select the new launcher group tab you want to add applications.
- 2 Select the **Launcher Group>Add Applications to Current Group...** menu item. You can also right click inside the group window and then select the **Add Applications...** from the menu.
- 3 Now select the applications you wish to add from the **Search for a Launcher** item window. Multiple applications can be selected by holding down the **Ctrl** key. Then click the **OK** button. The applications that are selected will now display in the new launcher group.

Note: Duplicate applications cannot be added to the same group.

Deleting applications from user created groups

- 1 Select the launcher group you want to delete applications from. Select the applications you want to remove from the group. You can select more than one application.
- 2 Select **Launcher Group>Delete Selected Items from Current Group** menu item. You can also remove applications by pressing the **Delete** button on the keyboard.

Note: Before deleting applications from the launcher group, the system will not display any confirmation message.

Renaming a Launcher Group

Follow these steps to rename a launcher group.

- 1 Select the tab you want to rename.
- 2 Select the **Launcher Group>Rename Current Group...** menu item. You can also access this option from the right mouse click menu.
- 3 You are prompted to rename the group. Enter the new name (up to 64 characters) and select the **OK** button. The group will now show its new name.

Arranging the icons of a Group

You can arrange the icons in each group separately.

- 1 Select **View>Arrange Icons by>Name** option. This will sort the icons alphabetically.
- 2 You can also select the auto arrange icons option. When auto arrange is turned off, the icons will stay where they were placed. Resizing the window does not change the position of the icons. There can also be space between icons. The Auto Arrange option is automatically enabled when a new tab is created.

Icon - Views

There are three different types of icon views:

- 1 **Icons** - This view will display with a 32x32 pixel icon with the caption underneath it. Icons can be dragged around in this view. This is the default view of a new group.
- 2 **List** - Icons will display with a 16x16 pixel icon to with the caption to the right of it. Icons will fill each column before going to the next. Icons cannot be dragged with this view.

Details - There are two columns in this view. Icons cannot be dragged with this view. Columns can be sorted by clicking the title of the column.

First Column - Icons will display with a 16x16 pixel icon to with the caption to the right of it.

Second Column -The description given to the launcher item in System Security.

To change the icon view, follow these steps:

- a) Select **View** menu group. You can also change the icon view by selecting the view buttons located next to the Log Out button.



- b) Select the appropriate icon view: Icons, List, or Details
- c) When auto arrange is turned on, the icons will automatically move to fit the window and there will be no gaps between icons.

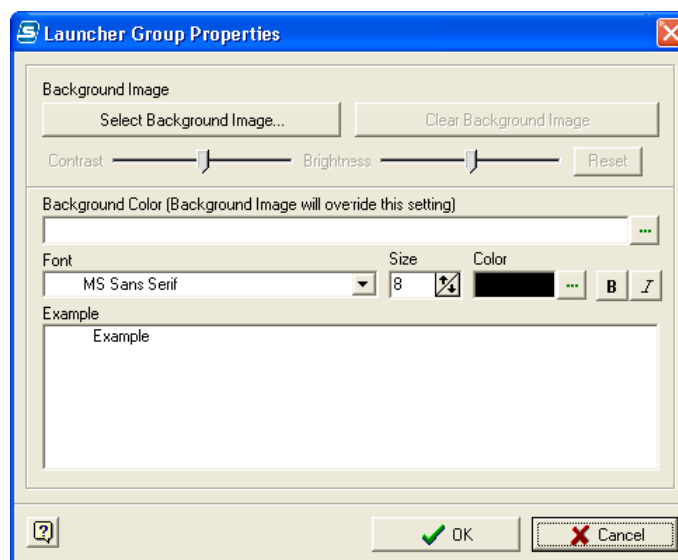
Launcher Group Properties

Each launcher group can have their own set of properties. These properties include:

- Background image
- Background color
- Font Style, color, and size

Follow these steps to setup the properties of a launcher group:

- 1 Select the Launcher Group menu group. Select the **Launcher Group Properties** menu item. Alternatively, you can right click on the group window and then select the Properties menu item. This will bring up the **Launcher Group Properties** dialog.



- 2 The first field in this dialog is the background image. The button **Select Background Image...** allows the user to search for an image file (*.bmp, *.gif, or *.jpg). Once an image is opened, the Example field at the bottom of the dialog will display the image. You can adjust the brightness and contrast of the image using the slider.
- 3 The **Clear Background Image** button clears the current image. The Example field at the bottom of the dialog will be updated with no background image.
- 4 The **Background Color** option is used to set the color of the group window.

Note: If a background image is selected, the background color will not be visible. The image overrides the color. Using the background color control will bring up a color palette, allowing the user to select any color they want. Once a color is selected, the 'Example' field at the bottom of the dialog displays the new color.

The next fields are the settings for the font of the icons. The font face, size, color and style can be selected using these options.

- 5 The font combo box displays all the fonts currently installed on the users system. The user can select any font they wish. The **Size** option changes the font size. Six is the minimum, twenty four the maximum, and eight is the default. The **Color** field changes the font color. This brings up the same dialog as the background color control.

Note: You should not pick a font color that cannot be seen easily because of the background image or background color. The example field towards the bottom should help the user select an appropriate color.

The font styles bold and italics can be changed by toggling the corresponding buttons. Any changes to the font will be displayed in the example control allowing the user to see what the changes will do before actually applying them.

- 6 Once the user is satisfied with the example shown, select the **OK** button. The Cancel button will exit the dialog without applying the changes.

Rearranging Launcher Group tabs

Launcher group tabs can be rearranged using a drag and drop approach.

- 1 Start dragging by selecting the tab you want to move.
- 2 Then drag the tab to the position you want to move it. It must be dropped onto the tab you want to change positions with. Release the mouse. The tabs should be in their new spots.

Recently Launched Applications

The launcher now keeps a list of the last ten applications launched in a recently launched drop down box for quick access. The combo box is part of the toolbar. The most recently launched applications are on the top.

To launch a recently launched application, follow these steps:

- 1 Select the application in the recently launched drop down box.



- 2 Click the lightning bolt button to the right of the drop down box.

Note: The lightning bolt icon to the left of the combo box launches the application selected in the group window.

- 3 Select the lightning bolt button to execute the application or select **File>Execute** option.
- 4 You can also access all recently launched applications by following these steps:
 - a) Select the **File>Reopen** menu group.
 - b) Select the application you want to launch.

Exiting Launcher

- 1 To exit the launcher window either select the **Exit the System Launcher** button or select **File>Exit** option.

Logging out of the system

Logging out the system prevents an unauthorized person from accessing the system at your security privilege level and ensures that the system attributes the operator activity to the correct operator. Logging out automatically closes every system function, except any open modules that are in the system start up window.

- 1 To log out from the system, click on the **Log Out** button on the launcher window. You will be prompted to confirm the action.
- 2 Click **Yes** log off or click **No** if you want to cancel logging off. After you log off, the system will prompt you with the **Log In** window. This indicates that your workstation is still active with modules running. You can access the applications at any time you want by logging into the system.

Note: Log out of the system when you leave the station unattended.

- 3 If you want to exit from the system, close the launcher window. You will be prompted to confirm the action.
- 4 Click **Yes** to exit from the system or click **No** to cancel the action.

Customer support

If you face any problems while installing this software, please contact the technical support for assistance.

Technical support help line - 866.322-1237

E-mail - schlegesms_techsupport@irco.com

Hours of operation

Our standard Technical Support hours are from 8.30 am to 5:00 pm Eastern Standard Time, Monday through Friday, excluding Ingersoll Rand observed holidays.

After hours calls and those placed on holidays will be directed to Technicians on a rotating basis. After dialing the main number, directions will be provided for contacting the technician(s) on duty at the time.

Registry Editor

CHAPTER 2

Introduction

The **Registry Editor** contains **Schlage SMS Registry Settings**. The five tabs are System Information, System Processes, Database Connection, Report Database Connection and Alarm Monitor. The original settings are entered during the Schlage SMS Software installation and can be modified using this module.

Note: As with any software product, incorrectly changing system settings can render your application inoperable. Please write down all settings from all tabs before modifying any fields. If you have any questions contact our Schlage Technical Support team.

This is a control module and only trusted **Schlage SMS Administrators** should be given privileges to access this module. Within these tabs are extremely important and confidential database criteria.

Accessing the application

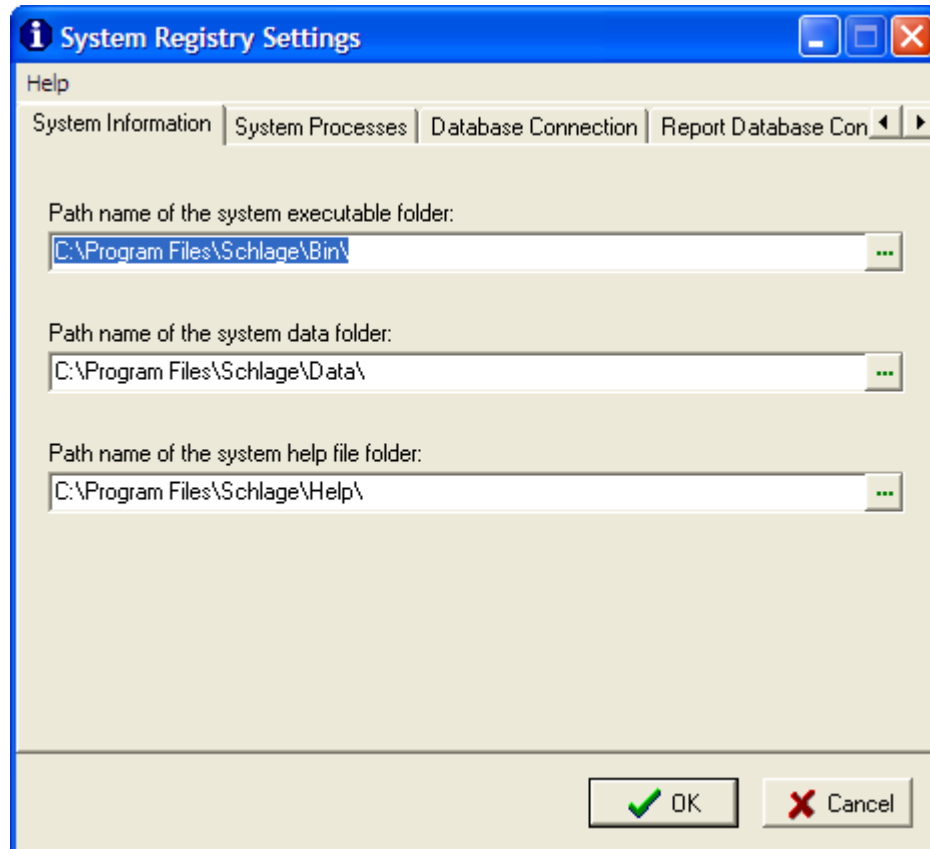
- 1 Select **Start>Programs>Schlage SMS>Registry Entry**.

Settings

When the module is opened, the System Registry Settings are organized under four tabs. Use the arrows to scroll through the four tabs. The default tab is **System Information** and it will remain active tab until a different tab is selected.

System Information

This tab contains the path and name of the **Schlage SMS** system folders. The example below shows the path of a single user system. With a Client/Server Installation, the Executable and Help folders generally will reside on the local workstation while the System Data folder resides on the server. To modify folder locations, use the expand button.

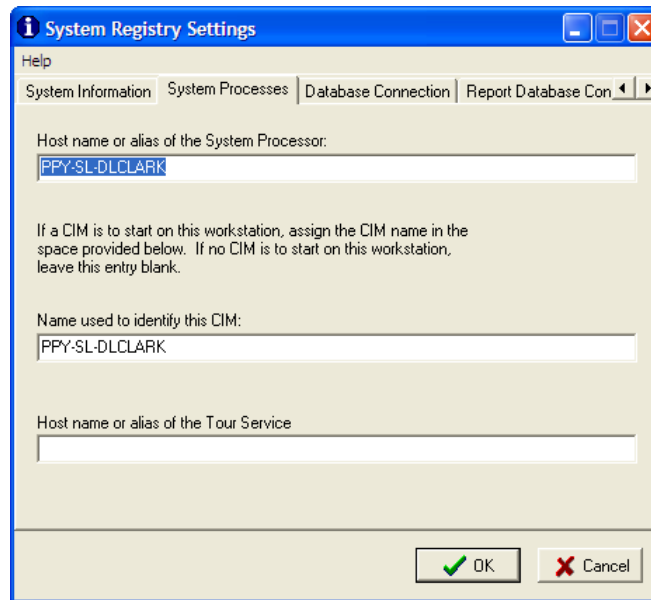


System Processes

The **System Processor**, **Communication Interface Module** and **Tour Service** names are identified here. These names are provided during the **Schlage SMS** installation and are also stored in the host file.

CIM names are also defined in the **System Manager** module.

You should also specify a host name or alias of the **Tour Service**. It is the name of the computer where the service is running.

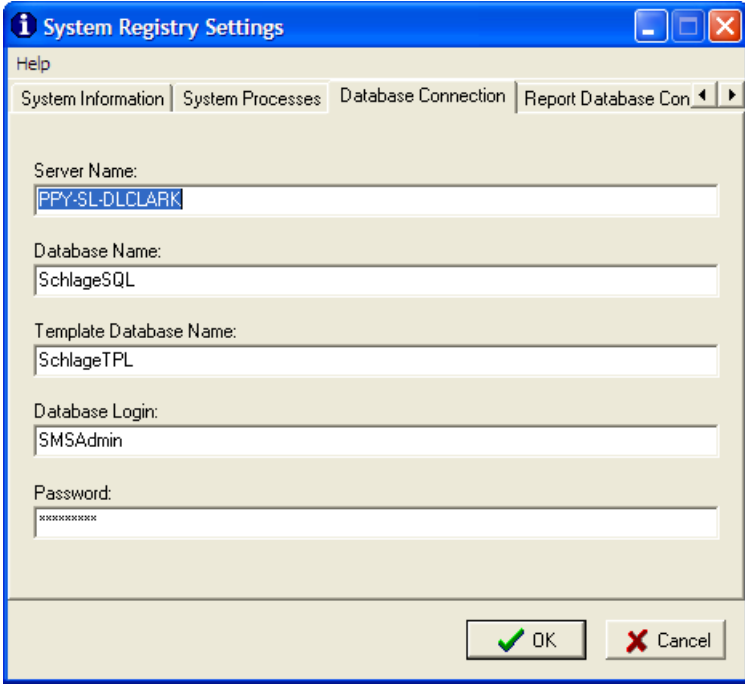


The image shows a Windows-style dialog box titled "System Registry Settings". It has a blue title bar with standard window controls. Below the title bar is a "Help" button and a tabbed interface with four tabs: "System Information", "System Processes" (which is selected), "Database Connection", and "Report Database Con". The main area of the dialog is light beige and contains three text input fields. The first field is labeled "Host name or alias of the System Processor:" and contains the text "PPY-SL-DLCLARK". Below this is a paragraph of text: "If a CIM is to start on this workstation, assign the CIM name in the space provided below. If no CIM is to start on this workstation, leave this entry blank." The second field is labeled "Name used to identify this CIM:" and also contains "PPY-SL-DLCLARK". The third field is labeled "Host name or alias of the Tour Service" and is currently empty. At the bottom right of the dialog are two buttons: "OK" with a green checkmark icon and "Cancel" with a red X icon.

Field Label	Value
Host name or alias of the System Processor:	PPY-SL-DLCLARK
Name used to identify this CIM:	PPY-SL-DLCLARK
Host name or alias of the Tour Service	

Database Connection

In the Database Connection tab, the Server Name, Database Name, Database Login, Database Password and Data Source are available. On a single-user system, use the local computer name as the server name. **Data Sources** are defined within your system; use the down arrow button to change the selection.



The screenshot shows a Windows-style dialog box titled "System Registry Settings". It has a blue title bar with standard window controls (minimize, maximize, close). Below the title bar is a "Help" button. The dialog features four tabs: "System Information", "System Processes", "Database Connection" (which is selected), and "Report Database Con". The "Database Connection" tab contains five text input fields: "Server Name" (containing "PPY-SL-DLCLARK"), "Database Name" (containing "SchlageSQL"), "Template Database Name" (containing "SchlageTPL"), "Database Login" (containing "SMSAdmin"), and "Password" (containing masked characters "XXXXXXXXXX"). At the bottom right, there are two buttons: "OK" with a green checkmark icon and "Cancel" with a red X icon.

Report Database Connection

The report setting information is stored in this tab. The **Report Data Source** can be different from the **Database Data Source** listed in the previous tab. For instance, it is possible to store all Crystal Report data in a separate location than that of the Schlage SMS software. However, in many instances SchlageODBC is both the Database Connection Data Source and Report Connection Data Source; use the down arrow to modify the field.

The screenshot shows a Windows-style dialog box titled "System Registry Settings". It has a blue title bar with standard window controls (minimize, maximize, close). Below the title bar is a "Help" button. The dialog features three tabs: "System Processes", "Database Connection", and "Report Database Connection", with the third tab being the active one. The main area contains four labeled text input fields: "Report Server Name:" with the text "PPY-SL-DLCLARK", "Report Database Name:" with the text "SchlageSQL", "Report Database Login:" with the text "SMSAdmin", and "Report Password:" with masked characters "XXXXXXXXXX". At the bottom right, there are two buttons: "OK" with a green checkmark icon and "Cancel" with a red X icon.

System Settings

CHAPTER 3

Introduction

This chapter explains the methods that the system administrators can use to implement and configure the settings for the **Schlage SMS**. These settings are configured through **System Settings** module. The purpose of these settings is to automate certain processes for devices, badge creation, image capture and handling, expiration indicators, area states and door types. It also provides the system administrator with additional levels of security and control. You may want to make selections depending on your work need.

Note: You need to close System Settings application after making any changes in the settings for the change to take effect.

Accessing the application

- 1 Open the **Schlage SMS** launcher by double clicking on the launcher icon on your desktop or go to Start>Programs>Schlage SMS>Schlage SMS. Enter your assigned user ID and password.

In the **System Launcher** (on page 42) window, double click on **System Settings** icon.

There are nine (9) different tabs available in this module to configure the default settings.

- General Settings
- Schlage SMS Image Settings
- Schlage SMS Signature Settings
- Credential Options and Pin Calculator
- Area States and Door Types
- Badge Printing Defaults
- Advance Search Settings
- Offline Credential Setting
- **Campus Lock Settings** (on page 460)

General Settings

The **General Settings** window has three sections; **Expiration Indicators**, **Default Programs** and **Devices and Back-up** options.

The screenshot shows the 'System Settings' window with the 'General Settings' tab selected. The window has a menu bar with 'File' and 'Help'. The main area is divided into several sections:

- Expiration Indicators:** Contains a label 'Days in Advance to Indicate Expiration' and a numeric spinner set to '0' with a note '(0 - Same Day)'.
- Default Programs and Devices:** Contains two dropdown menus: 'Default Image Capture Device' and 'Default Signature Capture Device', both set to 'From File'.
- Backup Options:** Contains a label 'Maximum backup files stored' and a numeric spinner set to '5'.
- Cardholder Definition Default Expiration Date:** Contains a checkbox labeled 'Use Default Expiration Date' which is currently unchecked.

At the bottom right, there are 'OK' and 'Cancel' buttons.

Expiration Indicators

- 1 **Days in Advance to Indicate Expiration** - The data entered in this field determines how many days in advance you want the system to notify you that a cardholder's access control rights expiration date is approaching. Specific color schemes are used to indicate the access control status.

For example, if you enter two (2) in this field, the color indicator changes from green to yellow two (2) days before the expiration date. Once the expiration date has passed, the access control information field displays in red. Indicators are found in the **Cardholder Definition** (on page 137) and **System Manager (on page 72)** modules.

Default Programs and Devices

Here you can pre-set the image and signature capture devices.

- 1 **Default Image Capture Device** - From the drop down menu, select **From File**, **From Twain Device** or **Flashbus MV**. While capturing cardholder portraits in **Cardholder Definition** (on page 137) program or **Guest Pass System** (on page 497), the device you choose here will be the default capture device. If you select the **From File** option, the system directs you to default file folders to choose a previously saved image file while adding cardholders.
- 2 **Default Signature Capture Device** - The menu options available here are **From File**, **From Twain Device**, and **From Schlage**. See the above option for details. While capturing cardholder signatures in the **Cardholder Definition** program or in the **Guest Pass System**, the device you choose here will be the default capture device.

Backup Options

- 1 **Maximum backup files stored** - Specify the number of backup files you want to store in the directory.

Cardholder Definition Default Expiration Date

The system allows the user to set a default expiration date for cardholder access. Select the check box **Use Default Expiration Date**. Using the calendar available from the drop down menu, choose a date that will be used globally for cardholder access expiration.

Schlage SMS Image Settings

The settings under this section are used for image editing and enhancement. This window is divided into two sections.

- **Image Handling** (on page 56)
- **General Image Capture Settings** (on page 57)

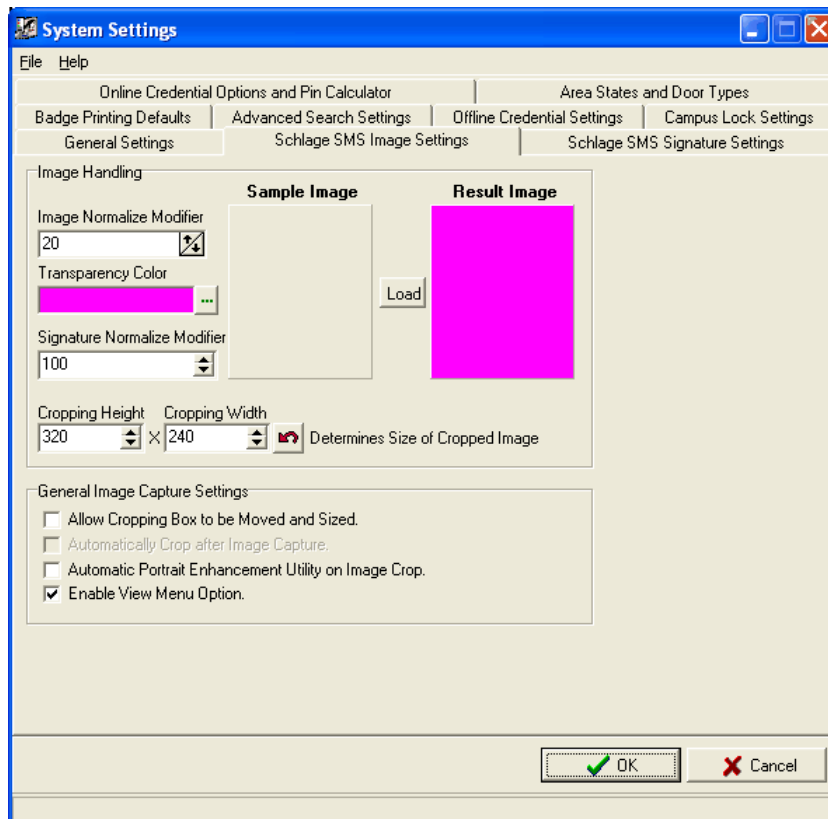


Image Handling

- 1 **Image Normalize Modifier** -The value entered here determines the number of background color levels that can be removed. The default is 20. This field is used when transparency is turned on for an image annotation.
- 2 **Transparency Color** - Click on the expand button to open the color palette. The color selected here will be used as the background color to show the transparency effect.
- 3 **Signature Normalize Modifier** -This option eliminates the halo pixels that surround a black and white signature. The recommended setting is 100.
- 4 **Cropping Height and Cropping Width** - Enter values for height and width of the cropping rubber band (crop box) in the empty fields.

General Image Capture Settings

- 1 **Allow Cropping Box to be Moved and Sized** - Cropping is a feature that enables portions of an image to be trimmed and removed from the original image. When this box is checked, the user can drag, resize and reshape the crop box. To activate the crop box in the Cardholder Image screen, click Show Cropping Rubber Band icon on the tool bar.

Drag and resize the crop box using the sizing handles located in the corners and along the edges of the red dotted lines. The Crop Box dimensions should match as closely as possible the height and width of the Cardholder Image Annotation that was created in the Badge Creation module. This reduces and removes any white space around the image on the badge.

To remove anything outside the red dotted lines, click the Crop Image icon on the tool bar. To save the location of the crop box in the **Cardholder Definition** program, right click within the crop box and select *Save Crop Box Location*.

- 2 **Automatically Crop after Image Capture** - Auto crop is used to select a portion of an image, then enlarge and crop it to create a new image. It will crop a portion of the original image and make that portion the new saved image when a picture is captured using a TWAIN device or FlashbusMV driver interface.

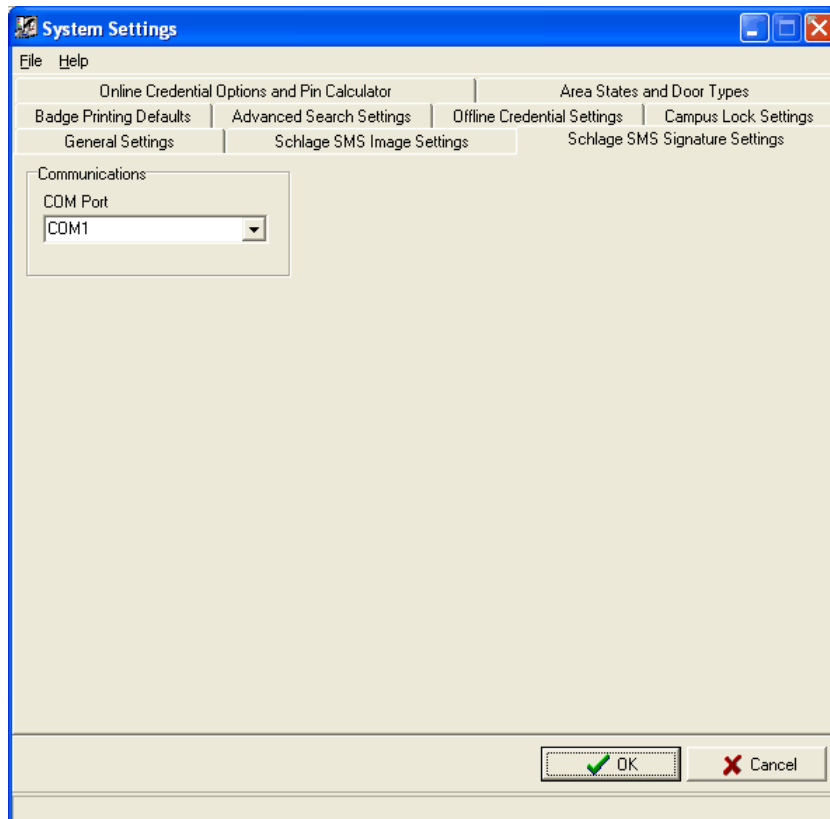
When using this feature, it is recommended that no checkmark be placed in the "Allow Cropping Box to be Moved or Resized". Once your crop dimensions have been saved (right click in **Image View** dialog box in the **Cardholder Definition** program and select **Save Crop Box Location**) turn the **Auto Crop** feature on by placing a checkmark in the box.

The Crop Rubber band will be in a fixed position. Use the Crop Image icon in the Cardholder Image screen in the **Cardholder Definition** program to create a new image. The cropped portion of the original image is contained within the red dotted lines.

- 3 **Automatic Image Enhancement Utility on Image Crop** - Place a checkmark next to this option to enable it. When a picture is cropped the Portrait Enhancement Utility displays 15 different views of the same portrait. The contrast feature can be adjusted by using the **Increase** and **Decrease** buttons on the bottom left section of the **Portrait Enhancement Utility** screen. To select one of these images, simply click in the picture.
- 4 **Enable View Menu Option** - Check this option to enable the View menu option to see the actual image in the Cardholder Image window.

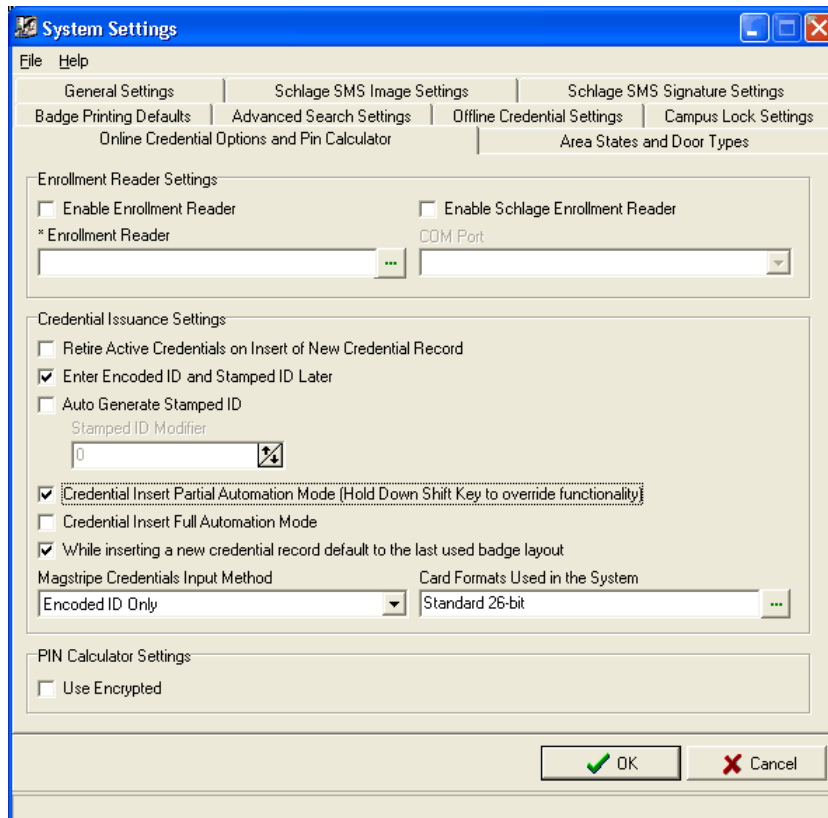
Schlage SMS Signature Settings

Click on the drop down menu to assign the signature pad's COM PORT (the port to which the signature pad is connected to capture the signature).



Online Credential Options and Pin Calculator

In this section you can find the settings for enrollment reader, credential issuance, and PIN calculator.

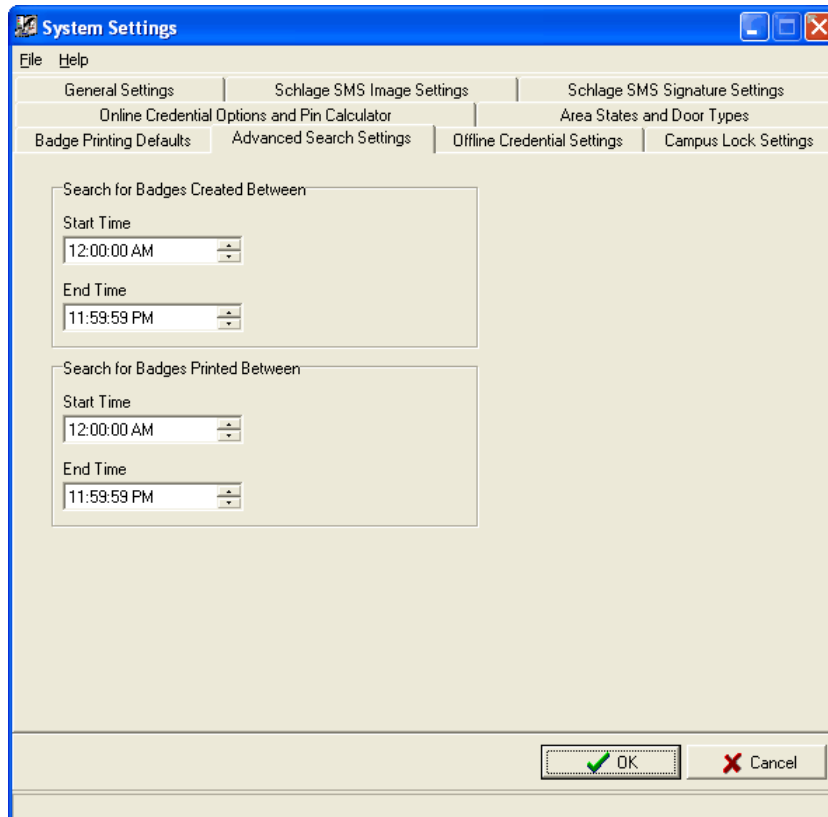


Enrollment Reader Setting

- 1 **Enable Enrollment Reader** - Check this option to retrieve the Encoded ID of a card and save it to the database using a reader device. This automated process is useful when multiple cardholders are being added to the system. The users can save time because additional keystrokes are avoided and it eliminates the possibility of typographical errors.
- 2 **Enrollment Reader** - Use the ellipse button to open the **Select Reader** sub window. Highlight the reader and click **OK** to assign the reader.

Advanced Search Settings

In this section you can set the start and end time of the badge creation and badge printing. The system uses this information when you perform advanced find functionality.



- 1 **Search for Badges Created Between** - The user can set the start and end time of the badge creation here. In the **Cardholder Definition** program, when the user performs an **Advanced Search**, the time set here will automatically appear in the related fields. The program defaults to 12 AM and 11.59 PM. When you run the query, the system will search, and display badges created between 12 AM and 11.59 PM during the dates you have specified here.
- 2 **Search for Badges Printed Between** - In the **Cardholder Definition** program, when the user performs an Advanced Search, the start and end time set here will automatically appear in the related fields. The program defaults to 12 AM and 11.59 PM. When you run the query, the system will search and display badges that are printed between 12 AM and 11.59 PM between the dates you have specified in the search criteria.

Credential Issuance Settings

- 1 **Retire Active Credentials on Insert of new Credential Record** - Check this option to enable the functionality to retire active badges when adding a new badge record. Retiring a credential takes away the access control privileges of that particular badge. This feature ensures security in case a cardholder loses his/her badge. This also prevents a cardholder from having more than one active badge at a time. The operator can retire the lost badge and assign a new badge to the cardholder. If you check this option, when you assign a new badge to an existing cardholder, a window pops up giving you an option to retire the existing credentials.

- 2 **Enter Encoded ID and Stamped ID Later** - This option allows the user to create a blank badge (a badge without an encoded ID and Stamped ID). In the Cardholder Definition program, while adding credential information the user gets an option to enter the encoded ID and Stamped ID later.
- 3 **Auto Generate Stamped ID** - Check this option to make the system generate the Stamped ID automatically.
- 4 **Stamped ID Modifier** - Enter a number in the empty field. When you assign a credential to a cardholder, the system calculates the Stamped ID or Encoded ID automatically. If you add Encoded ID, the system adds the value that you entered with the Stamped ID Modifier value and creates the Stamped ID. For example if your Stamped ID modifier is 10 and the Encoded ID is 250, your Stamped ID will be 260.

It works the opposite if you enter Stamped ID. In this case, the value will be subtracted from the Stamped ID modifier and creates the Encoded ID. For example if your Stamped ID modifier is 10 and the Stamped ID is 250, your Encoded ID will be 240.

Note: The **Stamped ID Modifier** feature will only work if the user is using the Encoded ID input method. This feature cannot be used with the Raw Data input method.

- 5 **Credential Insert Partial Automation Mode** - Place a checkmark in the box to enable partial automation feature. When the Add Credential option is selected on a new cardholder record, a blank credential record (a credential record without a Stamped ID and Encoded ID) will be automatically generated.

Note: In partial automation mode, Encoded ID and Stamped ID will not be generated, and must be entered manually. To enable the badge automation features, you need to first select the option **Enter Encoded ID and Stamped ID Later**. To generate badges automatically, you need to have a user-defined field linked to a badge technology and badge layout using **UDF Cross Reference** program.

- 6 **Credential Insert Full Automation Mode** - If this option is enabled, when you create a cardholder in the Cardholder Definition program, as soon as you capture a cardholder image a blank credential record is created.

Note: **Badge Insert Full Automation** feature also works in conjunction with the UDF Cross Reference Program.

- 7 **While inserting a new credential record default to the last used badge layout** - Selecting this option forces the system to default to the last used badge layout.
- 8 **Magstripe Credentials Input Method** - There are three options; Encoded ID Only, Raw Data Only, Encoded ID or Raw Data. See **Offline Credential Settings** section for more details on this option.
- 9 **Card Formats Used in the System**- Before creating any Magstripe or Proximity CM Credentials, the card formats used for these credentials must be selected here. Click on the expand button to add, delete and modify the card formats used in the system.

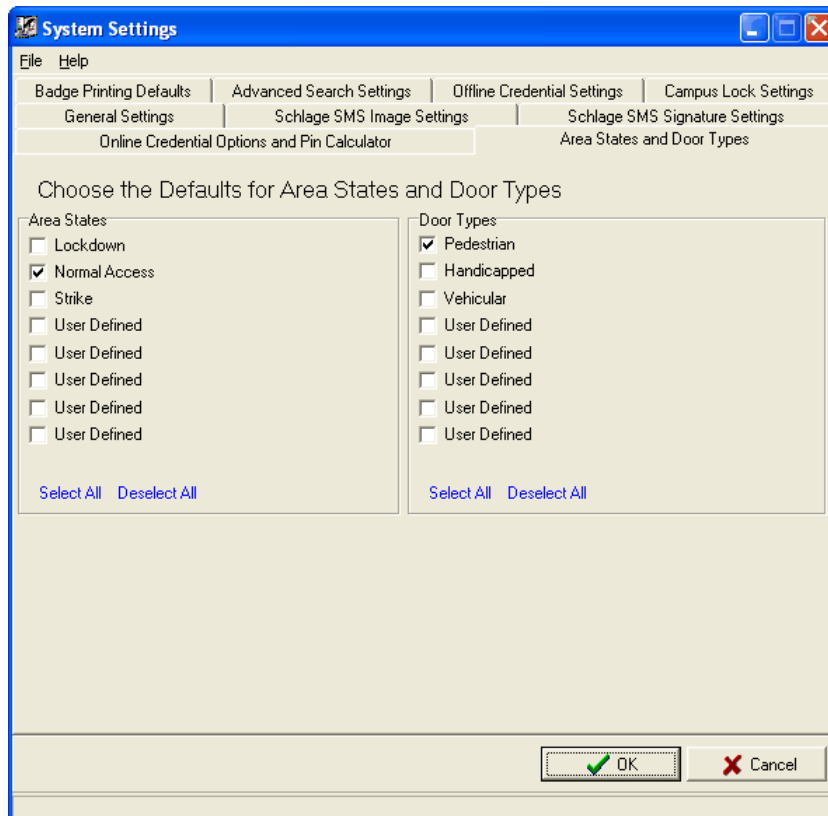
Note: For details on adding the card formats refer to the Offline Credential Settings section. Custom card formats can be created using **Card Format Editor** program.

Pin Calculator Settings

- 1 **Use Encrypted** - Check this option to automatically use Schlage Encryption to calculate a PIN for the Keypad ID field in the **Cardholder Definition** program. The encrypted number is based on the cardholder's Encoded ID number. If unchecked, the system will use standard encryption for the Keypad ID number.

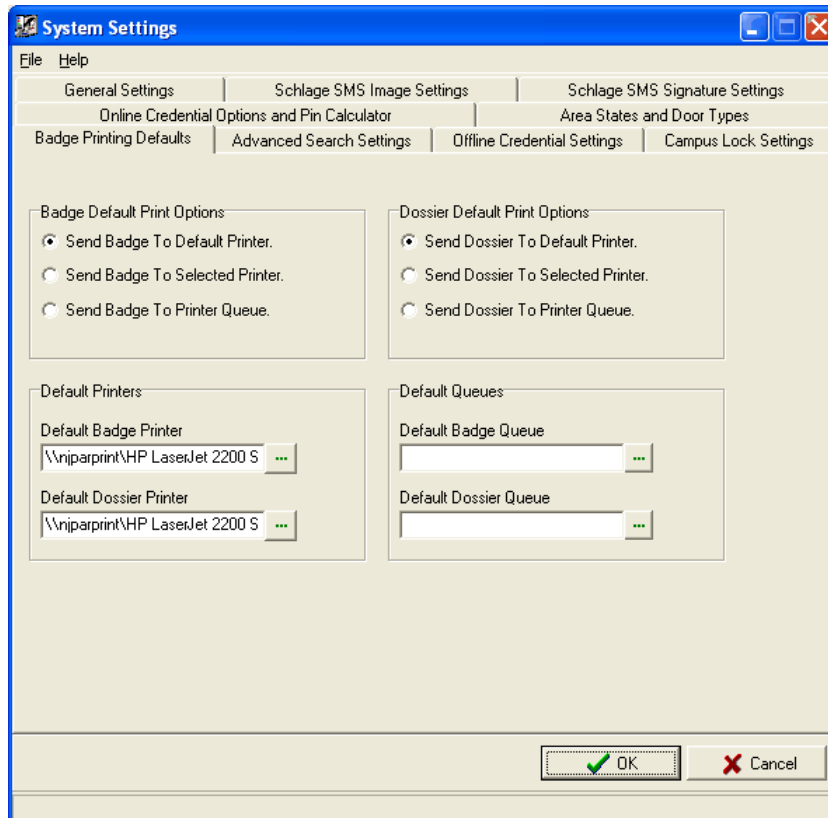
Area States and Door Types

This section provides a list of all the area states and the door types that have been defined in the database. The selections made in this window will set the defaults for Area Access Templates that are assigned to Areas and Area Sets in the System Manager program. Place a checkmark in the box to select individual items or use the buttons to Select All or Deselect All.



Badge Printing Defaults

This section contains the default badge print options and the default dossier print options. You can also set the default printers and queues.



Badge Default Print Options

- 1 **Send Badge To Default Printer** - Check this option to set a default printer for printing badges. Whenever the user prints a badge, the system will automatically send the data to the default printer.
- 2 **Send Badge to Selected Printer** - This option forces the user to select a printer from the list whenever you print a badge.
- 3 **Send Badge To Printer Queue** - In the **Cardholder Definition** program the user has an option to send the badge directly to the printer or a queue. This option allows you to send the badge to the queue and print later. Badge Queue is the module where badges are stored prior to printing. Badges in a queue can be printed individually or in batches.

Dossier Default Print Options

- 1 **Send Dossier to Default Printer** - This option allows the user to set a default printer for printing dossier reports. Whenever the user prints a dossier the system will automatically send it to the default printer.

- 2 **Send Dossier to the Selected Printer** - This option allows the user to select a printer from the list whenever you print a dossier.
- 3 **Send Dossier To Printer Queue** - In **Cardholder Definition** program, the user has an option to send the dossier directly to the printer or a queue. This option allows you to send the badge to the queue and print later.

Badge Queue is the module where dossiers are stored prior to printing. Dossiers in a queue can be printed individually or in batches.

Default Printers

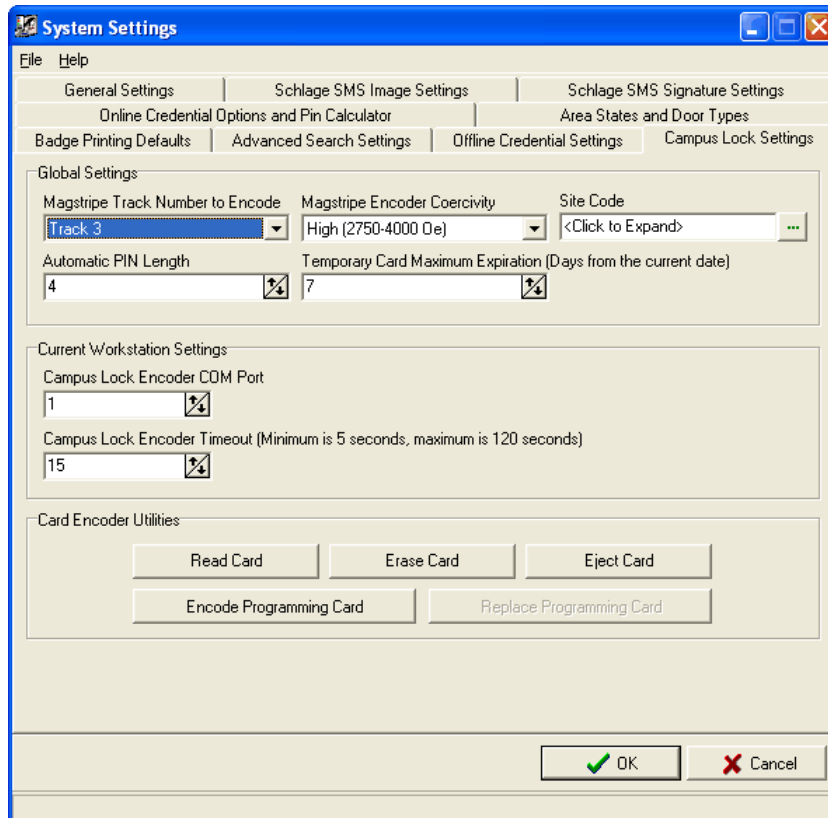
- 1 **Default Badge Printer** - Click on the expand button to set your default printer. If you have selected **Send Badge To Default Printer** option, whenever you print a badge, the system will send the data to the printer you have selected here.
- 2 **Default Dossier Printer** - Click on the expand button to set your default printer. If you have selected *Send Dossier To Default Printer* option whenever you print a dossier the system will send the data to the printer you have selected here.

Default Queues

- 1 **Default Badge Queue** - Click the expand button to select a queue for sending badges. The operator has to define queues using the badge queue program. Whenever the user sends a badge to the queue, the system will automatically send the data to this particular queue.
- 2 **Default Dossier Queue** - Click the expand button to select a queue for sending dossiers. The operator has to define queues using the **Badge Queue** program. Whenever the user sends a dossier to the queue, the system will automatically send the data to this particular queue.

Campus Lock Settings

Follow these steps to specify the campus lock settings. These settings need to be specified properly in order to encode a campus Magstripe card. Open the **System Settings** module. Select the tab **Campus Lock Settings**.



Global Settings

The first section is the global section. These settings are applied globally throughout the system, and can only be changed by an operator with administrative rights to System Settings.

- **Magstripe Track Number to Encode** - This is the track number of the Magstripe cards that the system uses while encoding a card. The user can select Track 1, Track 2 or Track 3.
- **Note:** The actual campus locks come pre-defined with a specific track so this setting must match their setting.
- **Magstripe Encoder Coercivity** - The three options in this drop down box are High, Medium, and Low with High being the default. This option must match the Magstripe badges the customer buys. Otherwise it will not encode properly and may damage the cards.
 - **Low coercivity** - As the name implies, low field energy is used to write data into the magnetic stripe of an ID card designed for low-energy encoding. Low-coercivity encoded cards are best used for medium-use, non-critical, security applications. One of the main benefits of using low-coercivity cards is the low cost.

- **High coercivity** - High-coercivity uses strong magnetic field energy to write data into the magnetic stripe of an ID card designed for high-energy encoding. High-coercivity encoded cards are best used in high-usage environments such as secured installations, where the long-life of the data on the magnetic stripe is of extreme importance. High-coercivity cards are resistant to data loss due to the high level of energy used to encode them. It is important to use the appropriate encoder-type printer with the appropriate coercivity cards. For example, if you use a low-coercivity encoder printer with high-coercivity cards, the field intensity created by the encoder will not be enough to permanently polarize the receptive material of the card. The magnetic stripe will rapidly lose its encoded information.

In the opposite case, in which a high-coercivity encoder is used with low-coercivity cards, the magnetic field created by the encoder will saturate the magnetic stripe of the card, rendering it useless, and the printer will not be able to verify the card.

- **Site Code** - Select a site code. You need to specify the site code before defining Campus Lock Credentials.
- **Automatic PIN Length** - This new field is used by Cardholder Definitions, when inserting a new Campus Lock credential. The PIN field will automatically be filled in with a random pin number with the length from the Automatic PIN Length field. The user can either use this PIN or enter a new one.
- **Temporary Card Maximum Range (Days from the current date)** - This setting is used within Cardholder Definitions when an operator wants to create a temporary campus lock credential for a cardholder. For example if this is set to seven (7), then the temporary card can be valid for seven (7) days from the date of issue. The minimum is one day and the maximum is thirty one (31) days.
- **Encode Programming Card** - This function is used to create a master credential that can be used to program CI locks (both legacy and AD250). Insert the card into the reader and click on the **Encode Programming Card** button. Once the card is successfully encoded, follow the instructions below to register the credential.

Instruction to Register a Programming Credential

For a legacy CL lock, follow the instructions below.

- 1 Open the back of the lock.
- 2 On the electronics board, press and release the **INI** button THREE times. The red LED will light and remain on.
- 3 Present the "master" credential to the reader. The green and red LEDs will alternately flash indicating acceptance.

For an AD250 CL lock, follow the instructions below.

- 1 Remove the lock's inside cover.
- 2 While pressing the **Inside Push Button**, press and release the **Tamper Switch** 3 times within 5 seconds. The **IPB** red led and left red Schlage LED will turn on.
- 3 Insert and remove a "master" magnetic stripe card into the lock. The IPB red LED and left Schlage red LED will turn off. The Schlage LEDs will toggle green / red 5 times to indicate acceptance of the master card.

Note: If the card was not a master credential, or was not read correctly, then the Schlage Red LEDs will flash 2 times, signifying that the master credential was not changed.

After manually programming the master credential, any previous master credential Card or default master PIN is deleted from the lock.

Current Workstation Settings

These will only take effect on the current workstation. These can be changed by operators who have Read/write permissions to System Settings application.

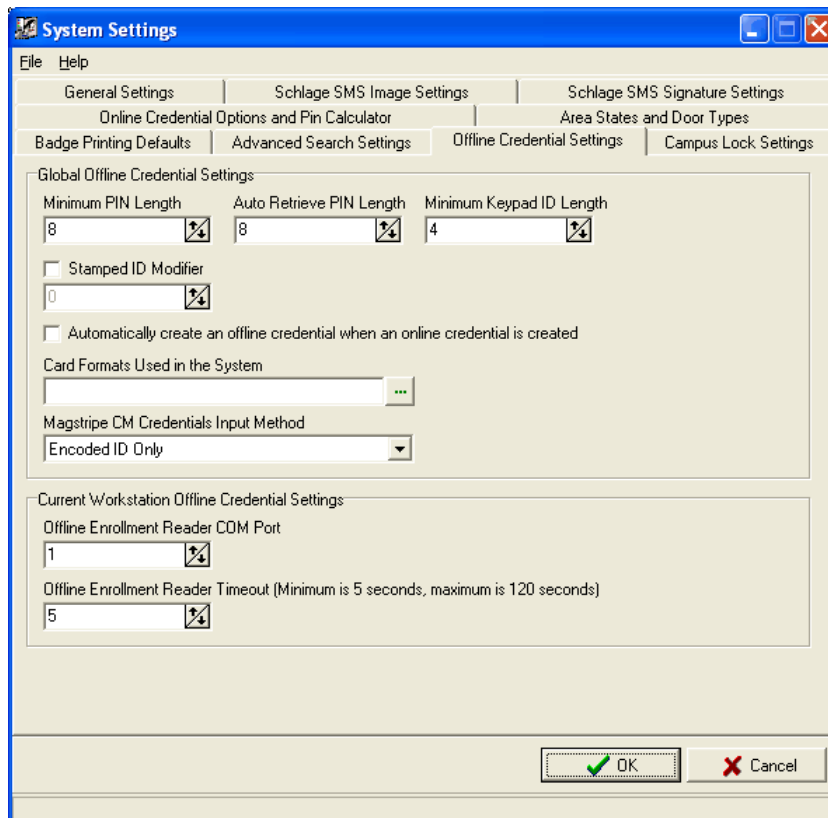
- 1 **Campus Lock Encoder COM Port** - Specify the COM Port the encoder is connected to. This only applies to workstations that have an encoder connected. Valid values are one (1) to two hundred and fifty five days (255).
- 2 **Campus Lock Encoder Time-out** - This is the amount of seconds it will take the encoder to time-out while waiting for a card to be placed into it. Valid values are five (5) to one hundred and twenty (120) seconds.
- 3 **Card Encoder Utilities** - This section has four different functions you can perform with the **Card Encoder**.
 - a) **Read Card** - Clicking this will read the track the system is using from a card that is placed into the encoder. The data will be displayed in XML format. Only operators with administrator permissions to this application can perform this operation.
 - b) **Erase Card** - This will completely erase a card that is placed into the encoder. It will erase all the tracks of the card. Only operators with administrator permissions to this application can perform this operation.
 - c) **Eject Card** - This option will take a card out from the encoder.
 - d) **Encode Programming Card** - This button is used to create the initial programming credential for campus locks or to create a duplicate programming credential.
 - e) **Replace Programming Card** - This button is used to replace old programming credentials with a new one. All old programming credentials will no longer work once this card has been swiped at the locks or the once the locks are re-programmed. This button will only be enabled in an initial programming credential was already created. After the programming credential is successfully encoded, the user is informed that they must register the credential at all locks that do not have it already registered.

Note: These buttons are only enabled if the user has administrator rights to System Settings.

Offline Credential Settings

The **Offline Credential Settings** contains two sections.

- **Global Offline Credential Settings** (on page 68)
- **Current Workstation Offline Credential Settings** (on page 71)



Global Offline Credential Settings

This section contains all the offline credentials settings that are applicable to the entire system.

Note: Only users with **Administrative** rights to the **System Settings** module are able to modify these settings.

- 1 **Minimum PIN Length** - This is the minimum PIN length a user can have when defining a PIN offline credential. The PIN Length can be between three (3) and eight (8) digits. The default is eight (8) digits. The following is a chart of the possible amount of unique PINs according to the PIN Length.

PIN Length	Possible amount of unique PINs
3	125
4	625
5	3125

PIN Length	Possible amount of unique PINs
6	15625
7	78125
8	390625

- 2 **Auto Retrieve PIN Length** - This is the length that an automatically generated PIN will use. You can now auto-generate PIN numbers in the **Offline Credential Definition** dialog in **Cardholder Definition** by selecting the credential technology as PIN, and then clicking the **Auto Retrieve** button. This feature will use the minimum PIN length specified here. The default is eight (8) digits.

Note: This setting applies only to PIN's; it does not apply to Keypad ID's.

- 3 **Minimum Keypad ID Length** - Specify the minimum length required for the Keypad ID. The value can be between 3 and 8 digits. The default is 4 digits.
- 4 **Stamped ID Modifier**- Enter a number in the empty field. When you assign a badge to a cardholder the system calculates the stamped ID or encoded ID automatically. If you add encoded ID, the system adds the value that you entered with the Stamped ID Modifier value and creates the stamped ID. For example, if your Stamped ID modifier is 10 and the Encoded ID is 250, your stamped ID will be 260. It works the opposite way if you enter stamped ID. In that case, the value you entered will be subtracted from the stamped ID modifier and creates the encoded ID. For example if your Stamped ID modifier is 10 and the Stamped ID is 250, your encoded ID will be 240.

Note: The Stamped ID Modifier will only work if the user is using the Encoded ID input method. If the user is using the Raw Data input method, then it will do nothing.

- 5 **Automatically create an offline credential when an online credential is created** - If this setting is enabled, when an online credential is created in the Cardholder Definitions program, a corresponding offline credential is also automatically created.

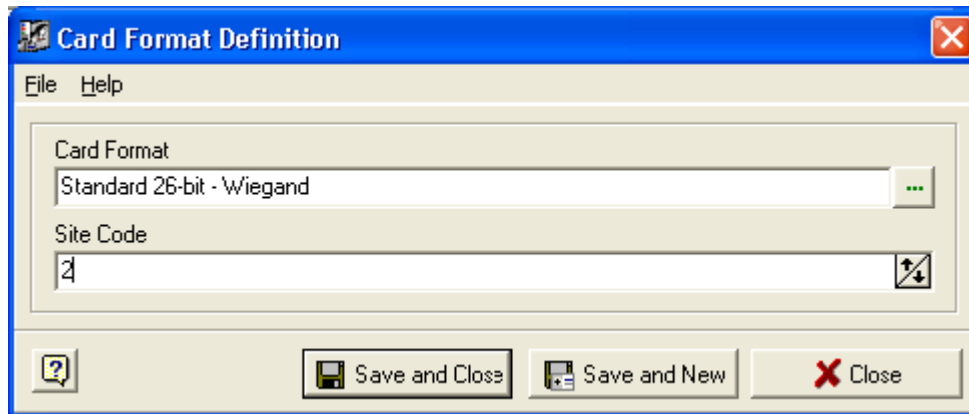
The following criteria must be followed in order for this feature to work:

- The above option in System Settings must be selected.
- The Encoded ID must be retrieved using the enrollment reader. After automatically retrieving the credential information, the user must not manually change Encoded ID, Credential Technology, and Issue Code.
- The user creates a new online credential with an Encoded ID using Cardholder Definitions. Keypad ID is optional. This feature will not work with credentials created with no Encoded ID.
- When the user saves the online credential using the Credential Definition dialog, the application verifies that the same cardholder does not already have an offline credential with the same Encoded ID and Keypad ID. If the user already has an offline credential that meets these criteria, then the process stops and no offline credential is created.
- If an Issue Code is in use by the online credential, it must be supported by the offline credential. If it is not supported, an offline credential will not be created and the user will be notified via an error message.
- The system verifies if the cardholder already has the same offline credential. If not, the system will attempt to create it. If an error occurs, the user will be notified of this error with a message explaining the reason why the auto offline credential creation feature failed.

Note: For further information on Magstripe template, refer to the System Manager chapter.

- 6 **Card Formats Used in the System**- This setting is used for creating proximity and Magstripe credentials for CM Locks. This helps the user to enter the Encoded ID manually.

- a) Click on the expand button, and all the formats used in the system are displayed. You can add, delete and modify the card formats used in the system.
- b) Custom card formats can be defined using the **Card Format Editor** program.
- c) To add a new Card Format Used in the System, select the browse button on the **Card Formats Used in the System** window.
- d) It opens the **Card Format Definition** window.



- e) Click on the expand button next to the Card Formats field. It opens the following window. Click on the + button on the toolbar to open the **Card Format Editor** window. Click the browse button, and the **Select a Card Format** window opens. Highlight and select a card format and click **OK**. The record appears on the **Card Formats Used in the System** window. Click **Close**. You can see the record in the **System Settings>Offline Credential Settings>Card Format Used in the System** field.
- f) You will not be able to select card formats that are already added. The available Proximity, Magstripe and Wiegand card formats are displayed. In the list of card formats, you will see a description and the badge format caption. Wiegand badge format is the same as proximity. Select the format you want to add and click **OK**.
- g) Once the card format is selected, you have the option of associating a site code with it. In the previous step, if you have selected a Proximity card format (Wiegand), you must enter a site code. To associate a site code, type in the site code value. To save the card format, just use the **Save** button.

If the site code field is left blank, the Encoded ID input method cannot be used. Only the raw data method or auto retrieving the credential will be allowed. Once the first Magstripe credential is created, the system will prompt you to save the site code extracted from that card for the card format.

The site code range will vary depending on the card format chosen. For example, if "Locknetic 16 digits mag card w/7-d site code" is chosen, then the site code can be between 0 and 9,999,999, but if "Schlage 34-bit – Wiegand" is chosen, the site code must be between 0 and 4095.

Once the card format and site code are entered, click **Save** to save the information in the system. The user can define as many card formats as they want, following the instructions above, but when multiple card formats are defined, the user must auto retrieve the Encoded ID using a CM Lock and a CIP. If only one card format is defined for proximity, the user can enter the encoded ID manually or use the auto retrieve method.

The same rule applies to Magstripe credentials. If only one Magstripe format is defined in the system, then the user can enter the Encoded ID, raw data, or use the auto retrieve method. If multiple Magstripe formats exist, then the user can only enter the raw data or use the auto retrieve option.

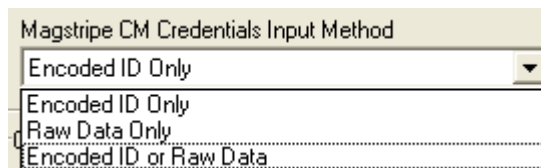
When defining multiple proximity formats, two formats with the same number of bits cannot be defined at the same time. For example, the format "HID 37-bit (16 bits for card id)" cannot be defined when the "HID/ProxIF 37-bit" has already been defined. You will get an error message.

- h) The same rule applies to Magstripe formats too. You cannot add two Magstripe formats with the same number of characters.

A brief note on site codes

Only one site code can be defined for a single card format. When creating credentials using the Encoded ID method, this site code will be used to construct the raw data for that card. If you happen to have the same card format with different site codes, you must use the auto retrieve option or enter the raw data for the card. If you use the Encoded ID method, the credential will receive the site code that was defined in the Card Format Definition window. If you enter the raw data or use the auto retrieve option, the system extracts the site code from the card. This is the reason why these methods allow different site codes.

- 7 **Magstripe CM Credentials Input Method** - This setting is used for creating CM lock credentials in Cardholder Definition. The drop down menu has three items. Encoded ID Only, Raw Data Only, and Encoded ID or Raw Data.



- a) **Encoded ID Only** - When this method is selected, the user can only enter the Encoded ID when creating Magstripe CM credentials in Cardholder Definition. The user will see the caption "Encoded ID" above the text box. For this method, you enter a small number, 10 digits or less, that is written on the card, usually on the back side. When the Encoded ID method is used, the raw data is automatically generated using the Encoded ID entered and the Site Code defined for that format (See section 1 above). The "Schlage Encoded Card" has the Encoded ID printed on the back. So this method should be used for those cards.
- b) **Raw Data Only** - When this method is chosen, the user will only have the option of entering the raw data when creating Magstripe CM credentials in Cardholder Definition. The user will see the caption "Raw Data" above the text box. For this method, you enter all the data from the Magstripe track. This will be a long string, up to thirty seven (37) digits, and can contain numbers and a few symbols. The "Locknetic 16 digits mag card w/7-d site code" has the raw data written on the front of it so this method should be used for those cards.
- c) **Encoded ID or Raw Data** - When this method is chosen, the user can use either of the above two options. The user will see two radio buttons on the CM Lock Credential Definition screen. One is for Encoded ID and one is for Raw Data. If Encoded ID is chosen, the user must enter the Encoded ID. If Raw Data is chosen, the user must enter the raw data. If the user enters the Encoded ID and then switches to the Raw Data method, the field is cleared and vice versa. However, there is one exception; if the user automatically retrieves the Encoded ID, and then switches to the Raw Data, the user will see the raw data for the card that was just auto retrieved and vice versa.

Note: The selection of the input method only applies while creating new credentials. When editing existing credentials, you can always see just the encoded ID.

Current Workstation Offline Credential Settings

- 1 **Offline Enrollment Reader COM Port** - Select the com port that the enrollment reader is attached.
- 2 **Offline Enrollment Reader Time-out** - This is used for auto retrieving the Encoded ID. If you don't swipe the card within the time frame specified here, the enrollment reader operation will be cancelled. You can set the time-out period as a value between 5 and 120 seconds.

System Manager

CHAPTER 4

Introduction

System Manager is a friendly tool that helps to integrate and categorize your unique company data as well as simultaneously monitor and maintain a secure working environment. It helps to define and setup your areas, time schedules, device locations, site codes, callback numbers and hardware which control access for all personnel. Special attention should be paid to security permissions assigned to this module in the **System Security** application.

Accessing the application

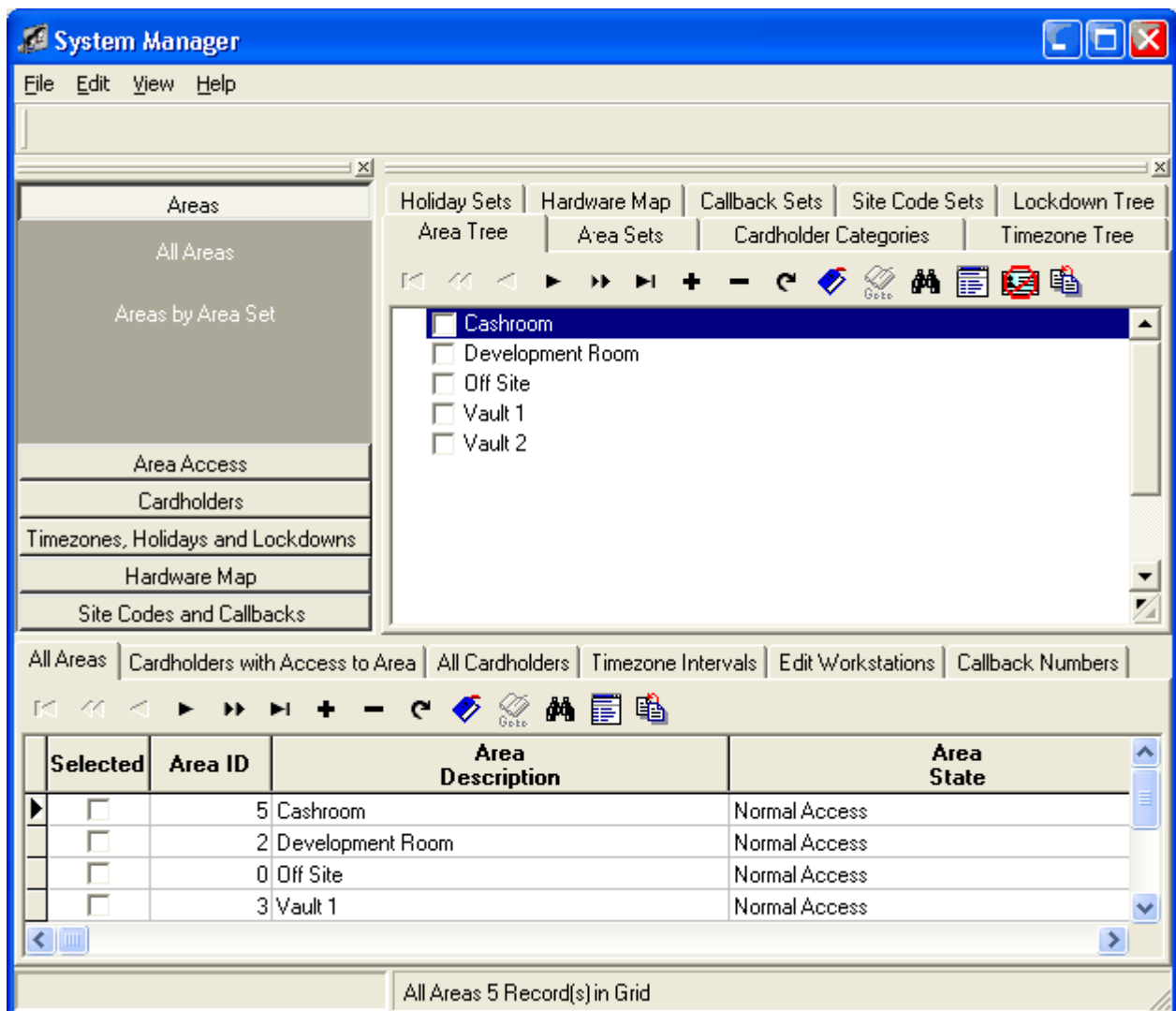
- 1 Open the **System Launcher (on page 42)** software by double clicking on the **Schlage SMS** icon on your desktop.
- 2 Enter your assigned user id and password. In the Launcher window, double click on the **System Manager** icon.

Working with System Manager

Overview

The System Manager's main screen is subdivided into three sections for ease of use as well as for the quick display of the specified characteristics of your data. The three sections are named the options bar, the tree view and the grid view. The options bar is located on the left side of the screen and contains shortcut buttons that quickly opens the tree and grid tabs that are associated with its topic.

These three sections are linked with each other; one section often necessitates definition and clarification in another section.



The six features available in the options bar are Area, Area Access, Cardholders, Time Zones, Holidays and Lock Downs, Hardware Map and Site Codes, and Callbacks. Selecting any one of these panels reveals a set of options that are linked to the other two window sections.

The next section is a set of tabs called tree window. Each tab of the tree displays descriptions. The plus icon prompts you to create new records. To move up and down the tree, use the arrow icons.

The bottom section of the System Manager is the information grid. This window consists of tabs that allow for the creation of the parameters of the definitions created in the tree grid. For example, as depicted above, if you wish to create a time zone interval that allows for security access every day of the week and all holidays, you can create the definition in the tree view and then specify the extent of that definition in the grid view. The status bar shows the total number of the records displayed in the grid.

The definitions created in the tree view often necessitate further description and parameters in the grid view. For instance, when you define a time zone in the timezone tree tab, verify that you have also completed the timezone intervals located in the grid view.

Note: Any programming method we show throughout the chapter may not necessarily be the only way to accomplish the respective task, but will probably be the easiest. As with all Schlage modules, there are several ways to accomplish the same task. The quickest way is to use the Options Bar feature which brings the appropriate tabs in the Tree and Grid windows forward. Drop down items are available under the Edit and View Menus, tabs are used to individually select Tree and Grid View windows. Hot keys are enabled.

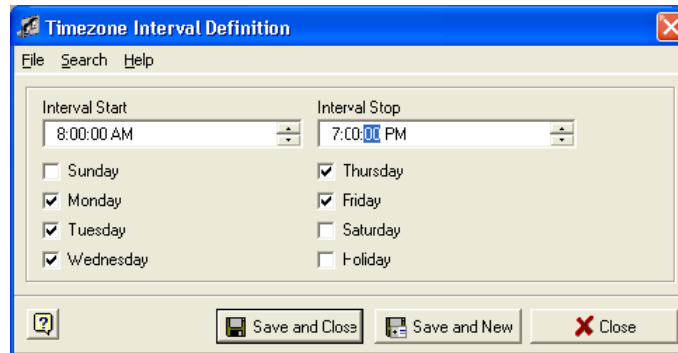
Timezone Intervals

The **Timezone Intervals** determine the cardholder's area access time. The system comes with two factory set time zones. The first one is *Always* which means 24 hours, 7 days a week, and Holidays, while the other one is *Never*, meaning access is allowed at no time and no days. Online system allows unlimited timezones, but for an offline system you can define only sixteen intervals per lock.

The fields with asterisks (*) are required fields.

- 1 To create a timezone, select Time Zones, Holidays and Lockdowns on the options bar.
- 2 Click on the **Timezone Intervals** button. The Timezone Tree tab in the tree view is brought forward as well as the timezone interval tab on the Information Grid.
- 3 Click the plus sign (+) on the time zone tree tab and add a timezone definition.
- 4 Click on **Save and Close** to save the definition and close the window and click on **Save and New** to save the definition and create a new one. Click on **Close** to exit the window without saving the definition.
- 5 click on the + sign on the information grid window to define a timezone interval.

- 6 Select the timezone interval and the days for the timezone definition. Here you set your **Interval Start** time and **Interval Stop** time (you can use the up and down arrows or enter the time directly in the fields) and select the individual days.



- 7 Click on **Save and Close** to save the definition and close the window and click on **Save and New** to save the definition and create a new one. Click on **Close** to exit the window without saving the definition. You can always modify the definition by double clicking on the record or by selecting the record and clicking the edit button on the tool bar. The change is reflected in the database.

You can define multiple intervals for a single timezone for the online system. The system does not allow you to define timezones that spans midnight (11.59.59 PM). The interval stops at 11.59.59 PM. The system will not allow access for a second, but you can define a second interval that starts at 12.00.00 AM. The number of intervals allowed for a timezone on an online system is unlimited.

Note: Offline locks support timezones with two intervals only if the timezone interval spans midnight on successive days. The first interval must stop at 11.59.59 PM and the second interval must start at 12.00.00 AM. Any other interval is invalid for offline locks. The timezones that are attached to offline locks can be modified, but system does not allow you to delete timezones that are attached to offline locks.

Areas and Area Sets

An **Area** is a space or group of spaces that have secured entry ways (e.g. door, gate and turnstile). An Area can consist of one reader or a number of readers and can be identified at one location or over several locations consists of door types and Area States.

Areas should be laid out as efficiently as possible. The layout depends on access privileges and the physical layout of the building. If there are three lobbies in your enterprise and all employees have access to all three lobbies, then it should be defined as one area such as the General Access Area or Main Lobby Area. These areas can have multiple readers, as the cardholders are given access to areas not to the readers. This avoids same cardholder records being downloaded to the controller board multiple times and thus wasting the memory space. The area access can be controlled based on timezone, door type and area state.

Areas have State and can be placed into any one of eight (8) states (normal, lock-down, strike and 5 user defined states.) **Area State** determines who has access to that area during a specific condition or state. For instance, if an area is placed in "strike", only those cardholders who have access during a strike are given access to the area. To change the name of an Area State or rename a user defined Area State, select the Area States from the Edit menu.

Area Access

Area Access tab is located in the options bar. This tab provides a way to view the cardholders and devices that are attached to an Area.

- 1 **Readers provide access to Areas** - To view the readers defined in the system by Area, click **View>Grid Windows>Devices>Readers by Area or Area Access>Readers Providing Access to Area**. There is no maximum limit to the number of readers that can provide access to the same area. However, you can only select one Area per reader when defining the reader device.
- 2 **Cardholders with access to an Area** - To view the cardholders who have access to an Area, select the Area and click on **Area Access>Cardholders with Access to Area or View>Grid Windows>Cardholders>Cardholders by Area**.

An **Area Access** record is generated for every cardholder permitted in the area. Cardholders are granted Area Access in several ways. The drag and drop feature is the quickest way to accomplish area access assignments. Cardholders can be dragged and dropped into Areas or an Area Set. Hold the control key down to make multiple selections. An Area or Area Set can be dragged and dropped into a cardholder category thereby granting every member of the category area access rights to a particular Area or to the Areas that are currently members of the Area Set.

Area Sets are groups of Areas to be used as an organizational tool. An Area can be in more than one Area Set. Area Sets determine the permissions the operators have over Areas. When an Area is created, it is automatically added to **All Areas** (factory set Area Set). Later, the administrator can assign it to the appropriate Area Sets as per your company needs. When you add a new reader to an existing Area, the reader will automatically have access to that Area.

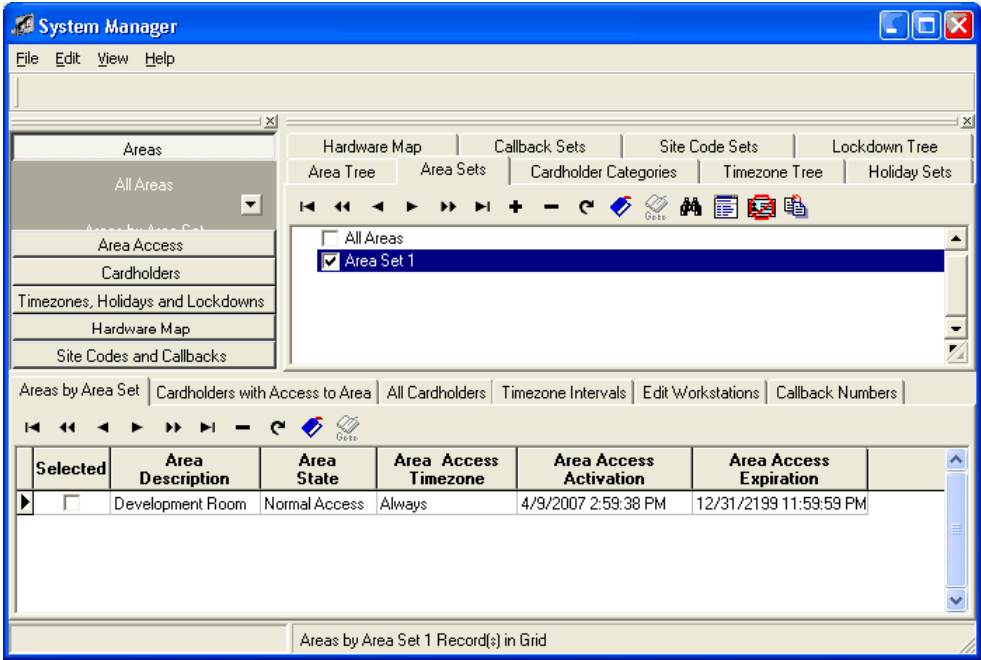
- 3 **Contacts attached to an Area** - To view the contacts attached to an Area, select the Area and click on **Area Access>Contacts attached to Area or View>Grid Windows>Devices>Contacts by Area**.
- 4 **Relays attached to Area** - To view the relays attached to an Area, select the Area and click on **Area Access>Relays attached to Area or View>Grid Windows>Devices>Relays by Area**.

Defining Area Sets

- 1 Click Areas on the option bar. The option bar for areas expands. Click on **Areas by Area Set**.
- 2 Click the + plus sign on the tree window. The **Area Set Definition** window opens. Enter an Area Set description and notes associated with it. The Description must be unique. Click **Save and New** for creating another area set or click **Save and Close** to complete the process.
- 3 To modify an **Area Set**, select the Area Set and double click on it or click on the **Edit** button from the tool bar.
- 4 To delete an area set, highlight it and press delete on the keyboard or click the - (minus) sign on the **System Manager** window. A confirmation message is displayed. Click **Yes** to continue and **No** to cancel the process.

Note: Deleting an area set will remove any access granted by a link to that area set.

The Areas by Area Set window displays, the Areas that belong to the selected Area Set and information regarding Area State, Timezone, Area Access Activation and Area Access Expiration.



Defining Areas

- 1 To define your Areas, click on the **Areas Panel** in the Options Bar, and click the + sign in the Area Tree tab. **Offsite** is an Area that is already pre-programmed by default (factory set).
- 2 Clicking the + sign opens the **Area Description** window. As an example, we can create an Area Definition called Lobby. The **Description** of the Area must be unique. Select the **Area Type**. You can select, Normal, Two Person Area (Scheduled), Two Person Area (Team). Refer to the **Two Person Rule** (on page 250) chapter to know more about this feature. The Area Type cannot be edited.

You will notice in this window, you can also select the Area State, which is a means of defining who can access that Area while it is in that state. In this instance, we will use the default state of **Normal Access**.

Add Area Wizard

Enter the Primary Data for this Area
A Description must be entered and an Area State must be chosen before you can continue.

* Description
Front Entrance

Notes

* Area Type
Normal

Maximum occupancy count
8

* Area State
Normal Access

? Cancel < Back Next > Finish

- 3 Click **Next**. In the next step define a template for area access. Select a Time Zone, Expiration Date and Time, and the Area States. When a cardholder is given access to this Area, an option is provided to use the template defined here.
 - a) Click **Next** to add a time zone for this Area.
 - b) Click on the down arrow to select the access activation and expiration dates. The calendar is displayed. Select a date. Using the up and down arrows change the activation and expiration time appropriately. The timezone, activation and expiration dates are applied based on what Area Set the Area is added to.

- c) Select the Area State and Door Type for this area. Click **Next** to continue, **Back** to go back to the previous step or **Cancel** to cancel the definition.

- 4 Select the **New Area's Initial Area Sets** window opens. Click on **Add Area Sets**. The **Search for Area Sets** window opens. Highlight the Area Sets you want to attach the area and click **OK**. Return to the window titled **Select Area Initial Area Set**. Click **Finish**.

Each Area can be assigned a stored template. Template values are unique for each Area copied to an Area Set. Each Area may have a separate and distinctive template every time it is assigned to a different Area Set.

Like this you can define as many Areas you like and attach them to area sets. Repeat the above steps to define another Area.

Copying Areas to Area Sets

At any time, you can supplement Area Sets with various Areas you have defined. This function is accomplished through **Copy Areas to Area Sets** wizard. (Edit>Copy Areas to Area Set) There are two modes to this wizard; **Basic mode** and **Advanced mode**.

Basic Mode

The basic mode lets you copy areas to area sets and creates an area access template that will be used for area access. In the basic mode all the areas copied to area sets uses same values for time zone, access activation and expiration time and dates, area states and door types.

- 1 Click on the **Copy Areas to Area Sets** button on the **All Areas** tab of the grid view section (**Edit>Copy Areas to Area Set**).
- 2 The **Select Area Sets** window opens. Click on **Add Area Sets** to select Area Sets that the Areas are copied.

Note: The **Change the wizard mode** button (this button is located at the bottom left corner of the window) allows you to choose between the basic and advanced modes.

Important: Changing the wizard from Advanced mode to Basic mode will clear all the selections.

- 3 Change the wizard to Basic mode.
- 4 Select the Area Sets you wish to copy the Areas. Click **OK**. The Area Sets you selected here are displayed in the **Select Area Sets** window. Now you can see that **Remove Area Sets** and **Next** buttons are enabled. Click **Next** to continue.
- 5 The **Select Areas** window opens. Click *Add Areas* to copy areas to area sets.
- 6 A window opens that allows you to select the Areas you want to add to the **Area Sets**. Select the Areas and click **OK** to continue. (Hold down the **Ctrl** key to select multiple Areas together.)
- 7 The Areas you selected here are displayed in the **Select Areas** window. Click **Next** to continue.
- 8 In the next step create an area access template. Click on the expand button to select a timezone for Area Access. Click on the down arrow to select access activation and expiration dates. Using the up and down arrows, select access activation and expiration time.
- 9 Select area states and door types. Click **Next**. A summary of your actions is shown in the next window. Click **Finish**.

Advanced Mode

The Advanced mode allows you to copy Areas to Area Sets and allows you to use an individual template for each area copied. This mode also helps the user to have different access record for each Area.

- 1 Follow step 1 in the basic mode section.
- 2 Change the mode of the wizard to Advanced. The following window opens. Click **Add Area Sets**.
- 3 A window displays the area sets you created. Select the area sets you want to attach the Areas. Click **OK**.
- 4 The area sets you selected are displayed in the **Copy Areas to Area Set** wizard. Highlight the area set into which you want to attach areas. The **Add Areas** button is enabled. Click on that button to select the areas to be added in the selected area sets. Click **OK**.
- 5 The Area Sets and areas you have copied are displayed. Click **Next**.
- 6 In the next step you can define the templates that will be used for all the areas copied to the area sets. In advanced mode you may use this template for the Areas or you have the option to use different templates for each Area. Choose the Area access time zone, expiration date and time, Area states and door types.
- 7 If you do not want to use the template values, click the back button to go back to the previous step. Highlight and select the Area that you do not want to use the template values.
- 8 The three buttons are enabled now. The first button helps you to set the template values, the second button allows you to use different area access values for each area copied to and the third button allows you to edit the area access permissions. Click on the second button to change the area access values. A message is displayed. Click **Yes** to continue.
- 9 The **Area Access Permissions** window is displayed. Click on the advanced button to expand the window. Make appropriate changes and click **OK**. Click **Finish** on the next window.

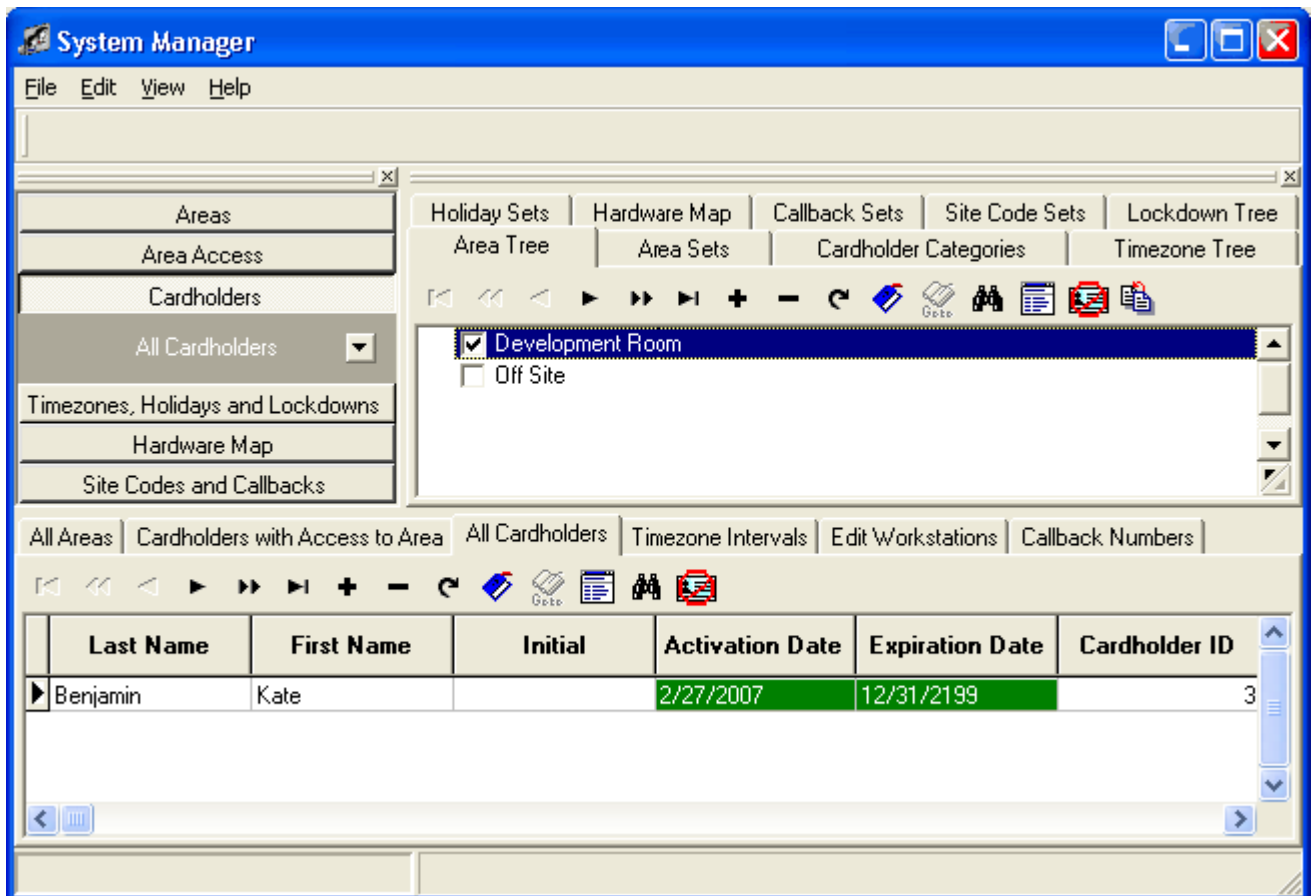
Cardholder with Access to Area

The user can run a search for cardholders by category or Area Access. The user can then take the results and add them to another area or area set using the drag and drop method. Follow these steps to drag and drop cardholders to areas and area sets.

- 1 Click on the **All Cardholders** tab located in the lower pane of the System Manager main window.
- 2 Click on the binoculars to search for cardholders.
- 3 In the **Advance Find of Cardholders** window, click on the button **Area Access** or **Categories**.

For example, here we have selected Area Access as our criteria. Click on **Add Area**. All the Areas defined in the system are displayed in a different window.

- 4 You can select the Areas by running a search and click **OK**.
- 5 Once you click **OK** on the **Select Areas** window, the Areas you selected will be added to the Search for Cardholders window. Click **Find Now**. All the cardholders attached with the selected Areas are displayed in the main window of the system manager.
- 6 Select and highlight the Area that you want to copy the cardholders. Then select the cardholders and drag and drop to the Area you selected.



Deleting Areas

- 1 If you want to delete an **Area**, select and highlight the areas you want to delete.
- 2 Click the delete button on your keyboard or click on the minus (-) sign on the System Manager main window. You get a confirmation message. Click **Yes** to continue.

You cannot delete the Areas that have cardholders or other devices attached to them. When you press delete, the program checks if there are devices and/or cardholders attached to them. A window pops up telling you exactly which devices and/or cardholders are attached. The Areas that cannot be deleted are automatically unselected from the grid. The Areas that do not have cardholders and/or devices attached will be deleted.

Holidays and Holiday Sets

Holiday Sets are a means of organizing access for employees on both standard workdays and holidays. Creating Holiday Sets is particularly useful for international corporations that may have multiple locations and thus need to recognize the different holidays of the countries they are in.

For example, a company with locations and employees in the United States and England will have to differentiate its holiday schedule and verify that its employees in England do not have access denied to them on the 4th of July which is a holiday for U.S employees.

You can create as many individualized holidays as necessary and thus set the kind and degree of access to any given employee.

- 1 To create a Holiday Set, click on the **Timezones and Holidays** tab in the **Options Grid** section. Then click on the **Holiday Sets** tab in the **Tree View** Section. Click on the + sign to define the Holiday Set.
- 2 For this example, we will create a Holiday Set named American Holiday Set. Click **Save and Close** to close the window or click **Save and New** to create another holiday set.
- 3 Now, you can define the holidays that are going to be associated with this **Holiday Set**.

Note: Menu and other buttons work in the same way as it works in the time zone definition. The advanced find feature allows you to save the search criteria and use it quickly at a later time. Right click on the record to select or deselect all the records.

- 4 Choose the **Holidays** tab under the Time Zone and Holidays panel in the Options Bar. This opens a tab in the Information Grid called Holidays. Click on the + sign and create a holiday definition for Thanksgiving.

- 5 Specify the start and stop dates of the defined Holiday. This feature is useful especially for corporations that have more than one consecutive day as holidays.

Note: This feature (specifying start and stop dates for a holiday definition) works only with SRCNX - 8 and SRCNX-16 controller boards which has firmware version 5.72 or greater. If the controller you are using does not support this feature, the system displays an error message.

- 6 Click on the down arrow to display the calendar. Choose the dates. Click **Save and Close** to close the window or click **Save and New** to define another holiday.

- 7 Then you will see your newly defined holiday for Thanksgiving appears in the Information Grid. Select Thanksgiving and drag it to the selected American Holiday Set above in the Tree Grid. You will be prompted with a confirmation message that asks "Are you sure you wish to copy the selected Holidays to the selected Holiday Sets?" Click **Yes**.
- 8 To verify that the holiday is in the holiday set, click on the newly defined holiday set in the Tree Grid section and then click on **Holidays** in the Options Bar and all the holidays for that set appears below in the Information Grid section.

You can also create all your holiday sets and holidays separately and then select and drag the Holidays from the Information Grid section to any Holiday Set you want them to go into in the Tree View Section. To move multiple records to a holiday set at the same time, select the records and hold down the right mouse click at the last selection. Then drag and drop the records to the Holiday Set.

Lockdowns

Lockdowns allow for a door to be secured Sunday to Saturday at a specific time. It only has one time interval. Cardholders will still be able to gain access based on their credential's offline function. A door that is in the lockdown state can be opened by sending an Automatic Override. This feature is currently available only for CM locks. A total of eight (8) lockdowns and automatic overrides can be added to a lock and may not be exceeded. Lockdowns cannot be duplicated on the same lock or an error message is displayed. The user can add or remove lockdowns to a lock.

- 1 To define a lockdown, select the Lockdowns from the **Timezone, Holidays and Lockdowns** tab. New lockdowns can be defined also from the CM Lock Definition window.
- 2 From the **Tree View** section, click the + sign to add a lockdown. The **Lockdown Definition** window opens.

- 3 Enter a definition for the lockdown and notes related to it. Select the **Lockdown Time** by using the up and down arrow. You can also enter the time directly in the field. Select the days by checking the boxes next the days. The door will be secured on the days selected here at the time you have specified. Click **Save and Close** to save the information and close the window. Click **Save and New** to save the information and define a new lockdown. Click **Close** to close the window and cancel the lockdown definition. The grid section displays the lockdown interval of the selected lockdown in the tree view.

Note: The system will not allow you to attach lockdowns with the same time schedule or overlapping schedule on offline locks. For example, if a lockdown is scheduled at 10 AM on Monday and Tuesday on Lock 1, you cannot again schedule a lockdown on that lock at the same time for Tuesday and Wednesday as there is a lockdown already scheduled at 10AM on Tuesday.

Editing Lockdowns

Lockdowns can be edited by double clicking on the record from the System Manager main window tree view. It opens the **Lockdown Definition** window; you can make modifications and save the record.

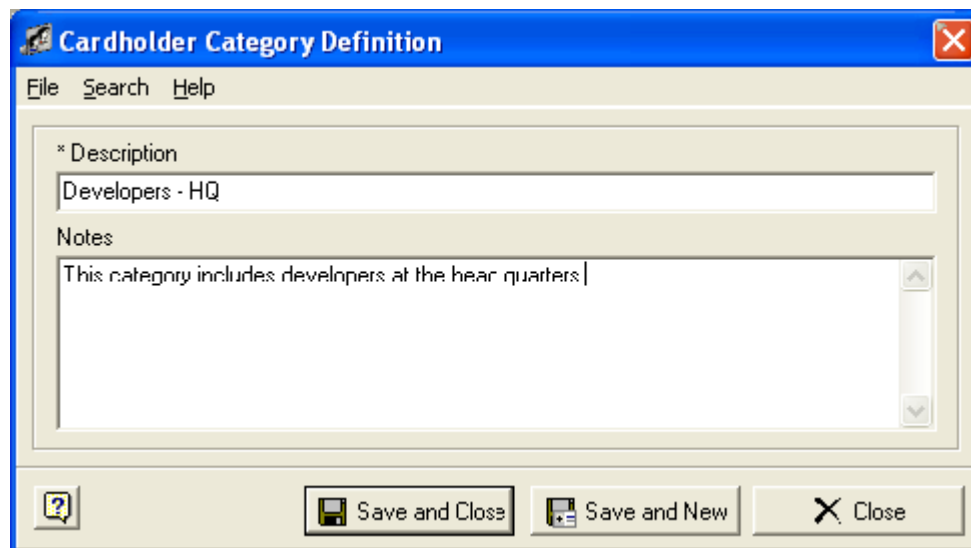
Deleting a Lockdown

The user can also modify or delete a lockdown from the tree view. To modify the information, double click on the record and the **Lockdown Definition** window opens. To delete the record, select the record and click the - sign from the tool bar. If the lockdown is attached to any lock, the system warns the user before deletion and prompts the user to confirm the deletion.

Cardholder Categories

Cardholder Categories allow the user to group the cardholders. This feature also works as a filter which allows users to find the cardholders and allow access easily.

- 1 Click on **Cardholder Categories** from the Options bar. Click the + sign on the tree window and Cardholder Category Definition window opens. Enter a description and the notes related to it. The Description of the category must be unique. Click **Save and Close** to complete the step or **Save and New** to define another call back number. Click **Close** to close the window without saving the definition.



Callback Numbers and Callback Sets

If you have a modem attached to a controller you need to define a callback numbers. When an alarm occurs, the controller calls the numbers that are defined as the callback numbers and the SP sends the alarm to the appropriate workstation. Call back numbers can be attached to callback sets. You can define multiple callback numbers to the same controller board and add them to a callback set. To define a callback set, follow these instructions.

- 1 Select **Site Codes and Callbacks** on the option bar. Click on **Callback Numbers By Callback Set** tab.
- 2 On the Tree window, click on **Callback Sets**. Click on the + icon. The **Callback Set Definition** window is displayed. Add the description of the callback set you are going to define. Add notes if any.
- 3 Click **Save and Close** to complete the step or **Save and New** to define another callback set. Click **Close** to close the window without saving the definition.
- 4 To add a callback number, click on the **Callback numbers** tab on the Options bar.
- 5 On the Grid window click on the add icon (+).
- 6 The **Callback Number Definition** window is displayed. Enter the description, notes and the phone number that you want the controller to dial. Click **Save and Close** to complete the step or **Save and New** to define another call back number. Click **Close** to close the window without saving the definition.
- 7 You can copy the callback numbers to callback sets using the drag and drop feature.

Site Codes and Site Code Sets

Every site can be assigned a number ranging from 1 to 1,000,000. Cardholders may be assigned one of these numbers for a specific site while the same number will not allow access to another site. Assigning site codes provides extra security that stops the cardholders with same encoded ID entering different sites.

When site codes are programmed and downloaded to the controller, the board checks for validity of that site code against the card that has been read. If the site code does not match with what is stored on the board, then access is denied to the cardholder. It can be used for readers that have been programmed for degraded mode. Degraded mode is used to continue to allow reader access when the controller board loses data communication with the reader interface. Therefore, lost communication does not interfere with access being granted because site codes are downloaded and retained in the reader interface memory.

Cards that are purchased from IR Security Technologies have the site codes encoded on the card.

- 1 To create site codes and site code sets, click on the **Site Codes and Callbacks** tab in the Option Bar section. Selecting **Site Codes** tab opens the **Site Code Sets** tab in the Tree Grid and the **Site Codes** tab in the Information Grid.
- 2 Select the Site Code Sets tab in the Tree Grid section and then click on the + sign to add a new site code set.
- 3 The **Site Code Sets** definition window opens. Enter the description and notes for your new site code set. For example create a Site Code Set called **Yourco**.

If you check the new **Yourco Site Code Set**, it will be highlighted and then ready if you choose to drag any Site Codes into it.
- 4 To create a site code, click on the **Site Code** tab in the **Options Bar** section and the **Site Code** tab on the **Information Grid** opens. Click on the + sign.

- 5 The **Site Codes Definition** window opens. Enter the description and notes for the new site code. For example, create a site code called Building One.

After you create your site codes, you can select them one by one and drag them from the Information Grid view section to the Tree View section and drop them on the Site Code Set you want them to belong. You get a confirmation message. Click **OK**.

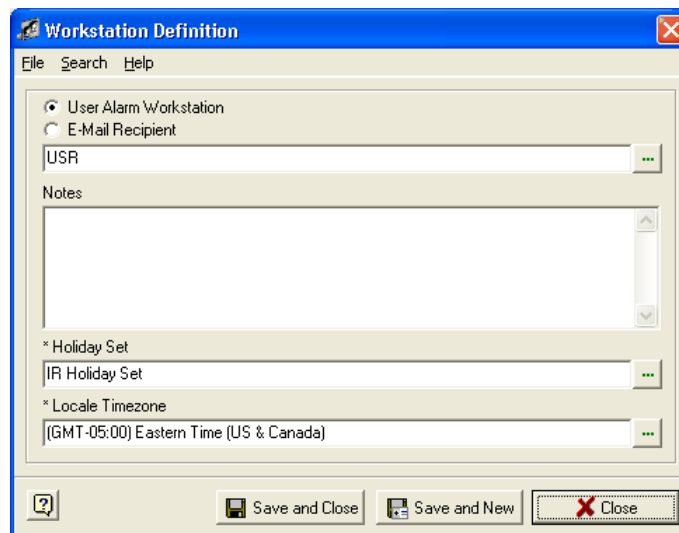
To select multiple site codes to drop in a site code set, first place a checkmark next to the Site Code Set. Then hold your control key down while highlighting the site codes. Drag the selected site codes and drop them in the site code set.

Hardware Definitions

The **Hardware Map** section is where you define your workstations, CIM (Communications Interface Module), CIM PORTS, Controllers, Readers, Contacts and Relays. The number of CIMs you need depends on how many transactions you will have and how many boards are connected. The CIMs are a determinant of the number of COM PORTS communicating and for that reason they are located on specific COM PORTS (such as CIM1 on COM1).

Define a Workstation

- 1 To define a workstation, select hardware map from the Options bar. Click on **Edit Workstations**. Click on the + Sign. The **Workstation Definition** window opens.



- 2 Select **User Alarm Workstation** to receive the alarms in the alarm monitor or the alarm graphics. The **E-mail Recipient Workstation** is where you receive the e-mails of alarms.

Note: E-mail settings are defined using the System Processor module. Please refer to System Processor chapter for further details.

- 3 Click on the expand button to select an operator. The operator's user id is inserted into the field.
- 4 Select a holiday set.
- 5 Select a time zone. Click **Save and Close** to complete the step or **Save and New** to define another workstation. Click **Close** to close the window without saving the definition.

Define CIM

- 1 To edit or create **CIM** information, click on the **Hardware Map** in the Option Bar and then select the **Edit CIM** tab. All the defined **CIMs** appears in the Tree Grid section on the Hardware Map tab. Click on the + sign or double click on a selected **CIM** to open the **CIM Definition** window.
- 2 Enter the description and notes for the **CIM**.

- a) Click on the expand button to select a location. This is the location where the **CIM** resides. When you click the expand button the **Select an Area** window opens.
- b) Select the number of I/O Port expansion.
- c) Select a holiday set and a host name. Enter the NetBios/machine name where the CIM applications will reside.
- d) Select the **Installed** check box to install this **CIM** in the system.

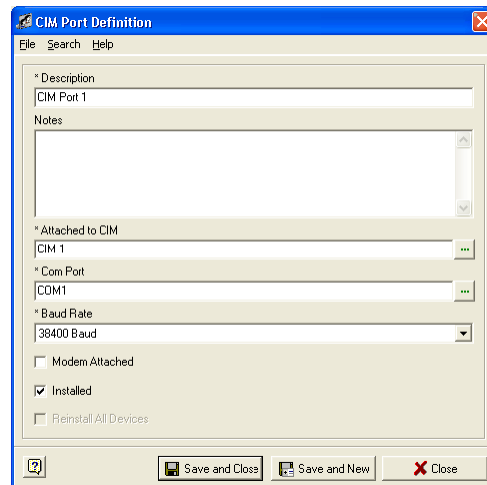
Note: Deselecting Installed check box uninstalls all the devices attached to this CIM.

- 3 If you have uninstalled the CIM, and want to re-install it, select the **Reinstall All Devices** check box. It will reinstall all the devices associated with this CIM.
- 4 Click **Save and Close** to close the window or click **Save and New** to define a new one. Click **Close** to close the window without saving the definition.

Define CIM Port

Now we need to define the CIM ports that the controller will use to communicate to the CIM.

- 1 To define the **CIM Port** information, click on the **Edit CIM Ports** tab in the Options Bar section. **CIM Port Definition** window opens.



- a) Enter a description and notes attached with it.
- b) Click on the expand button to select the CIM that is attached with this COM PORT.
- c) Select the COM Port that is communicating to the CIM, if you are using network for communication use the option "Network".
- d) Select the baud rate (communication speed) from the drop down menu.
- e) Select the check box if you are using a dial-up connection and you have a modem attached.
- f) Select the Installed check box to install this COM PORT.

Note: You need to always select the Installed check box. Deselecting this check box uninstalls all the devices attached to this CIM Port.

- g) If you have uninstalled the CIM PORT and want to re-install it, select the **Reinstall All Devices** check box. It will reinstall all the devices associated with this CIM PORT.

Define Controllers

- 1 To define a controller click on the Edit Controllers tab in the Option Bar. In the Information Grid the Edit Controllers tab opens. Click on the + sign. The Controller Definition window opens.

- 2 Enter a description and notes.
- 3 Click on the expand button to select the I/O port or master controller that the controller is attached. If you are defining a parent (master) controller select the I/O port. If it is a child, select the parent controller.
- 4 Select the location (Area) for this controller. This is used to identify the location of the controller for trouble shooting.
- 5 Select the controller model. E.g. SRCNX-16, SIONX24 etc. If you are using the expansion board for additional relays and contact points, select the SRCNX - 16 Expansion board.
- 6 If you are using a dial-up connection, select the callback set for this controller.
- 7 Select the site code set for this controller. Degraded mode works only if you specify the site codes. Degraded mode allows cardholders with specific site codes to access the areas even if there is a communication failure between CIM and the controller.
- 8 Select the holiday set.
- 9 Select the locale time zone.
- 10 If you are using network connection enter the IP address or host name.
- 11 Enter the IP port number.
- 12 If you are using a dial up connection enter the phone number.
- 13 Enter the master channel and board number.
- 14 Select the scheduled time zone (only if using model) for refreshing the controller memory automatically.
- 15 Network Device Type - If the controllers and workstations are communicating via network, specify the IP module you are using.

- 16 Administrative Password is used to login to the IP module to configure the module in the case of disaster recovery.
- 17 Access level Password - This is also is the password for the IP module.
- 18 Select the **Installed** check box.
- 19 Deselecting the Installed check box uninstalls all the devices attached to this controller.
- 20 If you have uninstalled the controller and want to re-install it, select the Reinstall All Devices check box. It will reinstall all the devices associated with this controller.
- 21 Click **Save and Close** to close the window or click **Save and New** to define a new controller. Click **Close** to close the window without saving the definition.

Scheduled Updates for Controllers

This feature lets you schedule automatic updates for dial-up controllers at specific time zone intervals. To program this feature, first you have to define a time zone. After defining the time zones, configure controllers that you want to update automatically. This feature works hand in hand with the CIM and the Controller. The CIM dials up the controller at scheduled intervals.

Follow these steps to program Scheduled Updates for controllers.

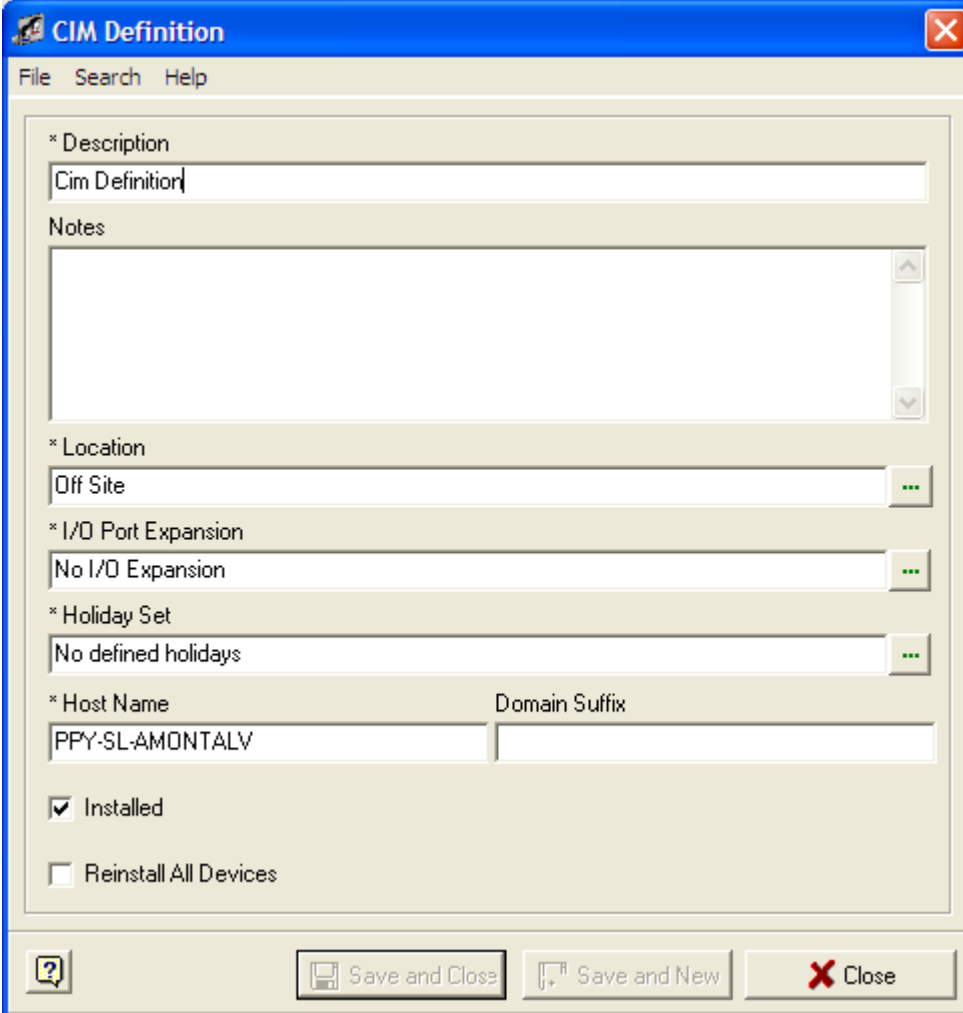
- 1 Define a time zone in the System Manager.
- 2 Assign Intervals.
- 3 In the **System Manager**, click on the **Hardware Map** button.
- 4 Edit the **CIM PORT Definition** window. Make sure that the *Modem Attached* check box is checked.
- 5 Select the dial up controller. Edit the **Controller Definition** window.
- 6 Enter the phone number for the scheduled updates. Select the time zone that you have defined for the scheduled updates. Each dial up port on the CIM checks the time zone on a regular basis. When a timezone goes active, the CIM PORT checks each of the controllers attached to that CIM PORT to find out whether its dial-up controller is scheduled for update during that particular time zone. Controllers scheduled for update on that time zone are queued for dialing. Each **CIM PORT** begins dialing whenever there are controllers in the dialing queue and the modem is not in use. The **CIM** simultaneously dials on all dial-up ports.
- 7 Click **Save and Close**.

Define SSRC

The SSRC Single Door controller is both a controller and a reader in one. To set up the SSRC the user will need to first set up the controller aspects and then the reader aspects.

To define an SSRC:

- 1 Set up your CIM Definition



The screenshot shows a window titled "CIM Definition" with a menu bar containing "File", "Search", and "Help". The window contains several fields and checkboxes:

- * Description:** A text field containing "Cim Definition".
- Notes:** A large, empty text area with a vertical scrollbar.
- * Location:** A text field containing "Off Site" and a green ellipsis button to its right.
- * I/O Port Expansion:** A text field containing "No I/O Expansion" and a green ellipsis button to its right.
- * Holiday Set:** A text field containing "No defined holidays" and a green ellipsis button to its right.
- * Host Name:** A text field containing "PPY-SL-AMONTALV".
- Domain Suffix:** An empty text field.
- ☒ **Installed**
- ☐ **Reinstall All Devices**

At the bottom of the window, there is a toolbar with three buttons: a question mark icon, a "Save and Close" button, a "Save and New" button, and a "Close" button with a red X icon.

- 2 Define your CIM Port Definition

CIM Port Definition

File Search Help

* Description
Network Port

Notes

* Attached to CIM
Cim Definition

* Com Port
Network

* Baud Rate
N/A

☐ Modem Attached

☒ Installed

☐ Reinstall All Devices

? Save and Close Save and New Close

- 3 Add your SSRC controller and attach to the CIM port definition. Use the new controller model: **SSRC Single Door Controller**.

Note: Make sure the SSRC has been configured on the network prior to entering the values here. See the installation manual for details.

Controller Definition

File Search Help

* Description
Single Door Controller

Notes

* Attached To I/O Port or Master
Network Port ...

Location
Off Site ...

* Controller Model
SSRC Single Door Controller ...

Callback Set
No callback numbers ...

Site Code Set
No defined site codes ...

Holiday Set
No defined holidays ...

* Locale Timezone
(GMT-05:00) Eastern Time (US & Canada) ...

IP Address or Host Name
10.45.49.78

IP Port Number
3001 ...

☐ Encrypted

Phone Number

Master Channel
N/A

Board Address
N/A

Schedule Timezone
Never

Network Device Type
Schlage SIPRCNX ...

Administrative Level Password

Access Level Password

Domain Suffix

☒ Installed

☐ Reinstall All Devices

Save and Close Save and New Close

- 4 Add a SSRC Reader and attach it to the SSRC controller.

Note: The SSRC template can be used to create all triggers, action items, AROs and MROs.

Reader Definition

File Edit Search Help

* Description
SSRC Reader

Notes

* Attached To
Single Door Controller

* Provides Access To Area
Area 1

* Reader Model
SSRC Reader

* Reader Type
Standard Reader

* Door Type
Pedestrian

Antipassback Time (Minutes) Channel Number Reader Address
0 1 1

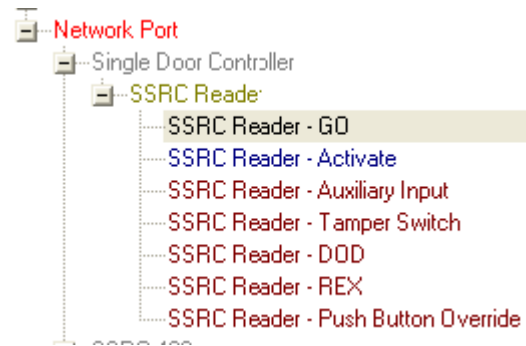
Reader Template
SSRC Reader

☐ Keypad Reader ☒ Degraded Mode ☐ Auto Relock
☐ Guest Sign In Reader ☐ Guest Sign Out Reader
☒ Installed
☐ Reinstall All Devices

Save and Close Save and New Close

- 5 Once defined, click on the **Save and Close** button.

Below is an example of the SSRC Reader Definition if the template has been used:



Define SSRC-300

The SSRC-300 is a variant of the SSRC. Instead of a single door controller, the SSRC-300 controls up to 8 Schlage AD-300 locks.

To define an SSRC-300:

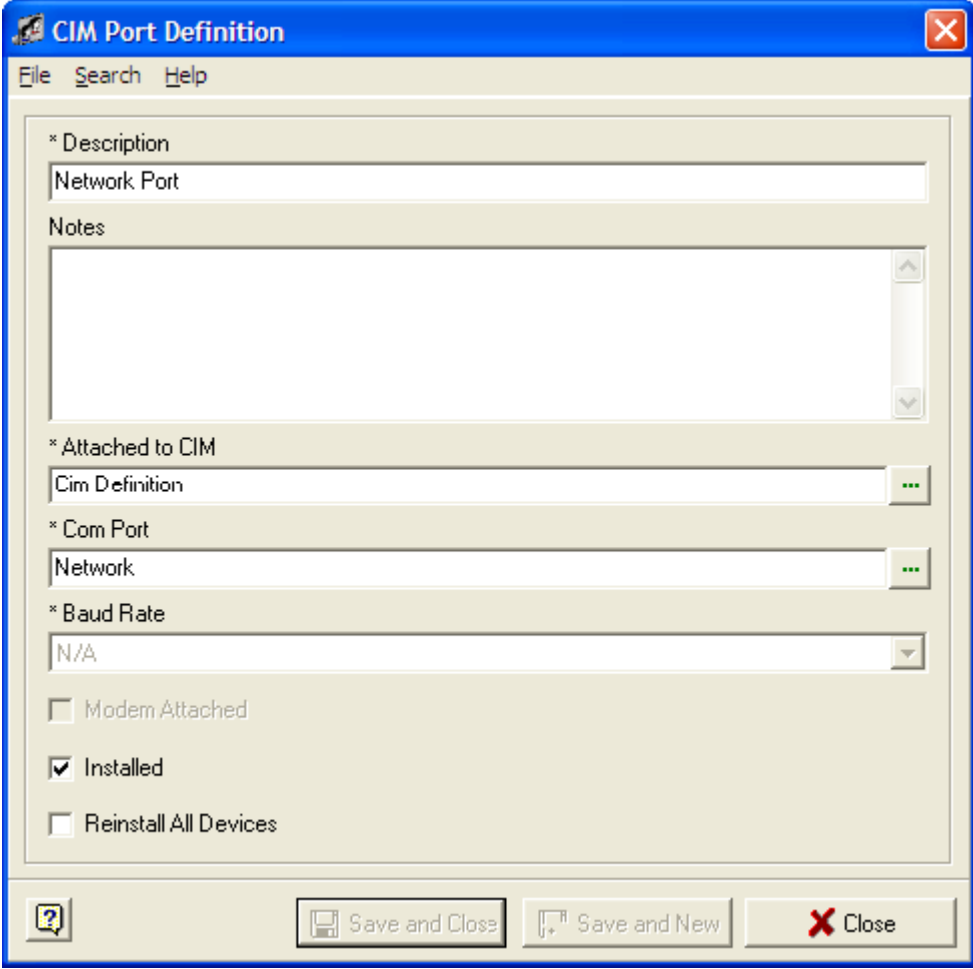
- 1 Set up your CIM Definition

The screenshot shows a Windows-style dialog box titled "CIM Definition" with a blue title bar and a red close button. The dialog has a menu bar with "File", "Search", and "Help". The main area contains several fields and checkboxes:

- * Description:** A text box containing "Cim Definition".
- Notes:** A large empty text area with a vertical scrollbar.
- * Location:** A text box containing "Off Site" and a green ellipsis button.
- * I/O Port Expansion:** A text box containing "No I/O Expansion" and a green ellipsis button.
- * Holiday Set:** A text box containing "No defined holidays" and a green ellipsis button.
- * Host Name:** A text box containing "PPY-SL-AMONTALV".
- Domain Suffix:** An empty text box.
- ☒ **Installed**
- ☐ **Reinstall All Devices**

At the bottom, there is a toolbar with three buttons: a help icon, "Save and Close", and "Save and New" (with a plus icon), followed by a red "X" button labeled "Close".

- 2 Define your CIM Port Definition



The screenshot shows a Windows-style dialog box titled "CIM Port Definition". It has a menu bar with "File", "Search", and "Help". The main area contains several fields and checkboxes:

- * Description: A text box containing "Network Port".
- Notes: A large empty text area with a vertical scrollbar.
- * Attached to CIM: A text box containing "Cim Definition" and a green ellipsis button.
- * Com Port: A text box containing "Network" and a green ellipsis button.
- * Baud Rate: A dropdown menu showing "N/A".
- ☐ Modem Attached
- ☒ Installed
- ☐ Reinstall All Devices

At the bottom, there is a toolbar with a help icon, a "Save and Close" button, a "Save and New" button, and a "Close" button with a red X icon.

- 3 Add your SSRC-300 controller and attach to the CIM port definition. Use the new controller model: **SSRC-300**.

Note: Make sure the SSRC has been configured on the network prior to entering the values here. See the installation manual for details.

Controller Definition

File Search Help

* Description
SSRC300

Notes

* Attached To I/O Port or Master
Network Port ...

Location
Off Site ...

* Controller Model
SSRC-300 ...

Callback Set
No callback numbers ...

Site Code Set
No defined site codes ...

Holiday Set
No defined holidays ...

* Locale Timezone
(GMT-05:00) Eastern Time (US & Canada) ...

IP Address or Host Name
10.45.49.17

IP Port Number
3001 ☒ Encrypted

Phone Number

Master Channel
N/A

Board Address
N/A

Schedule Timezone
Never

Network Device Type
Schlage SIPRCNX ...

Administrative Level Password

Access Level Password

Domain Suffix

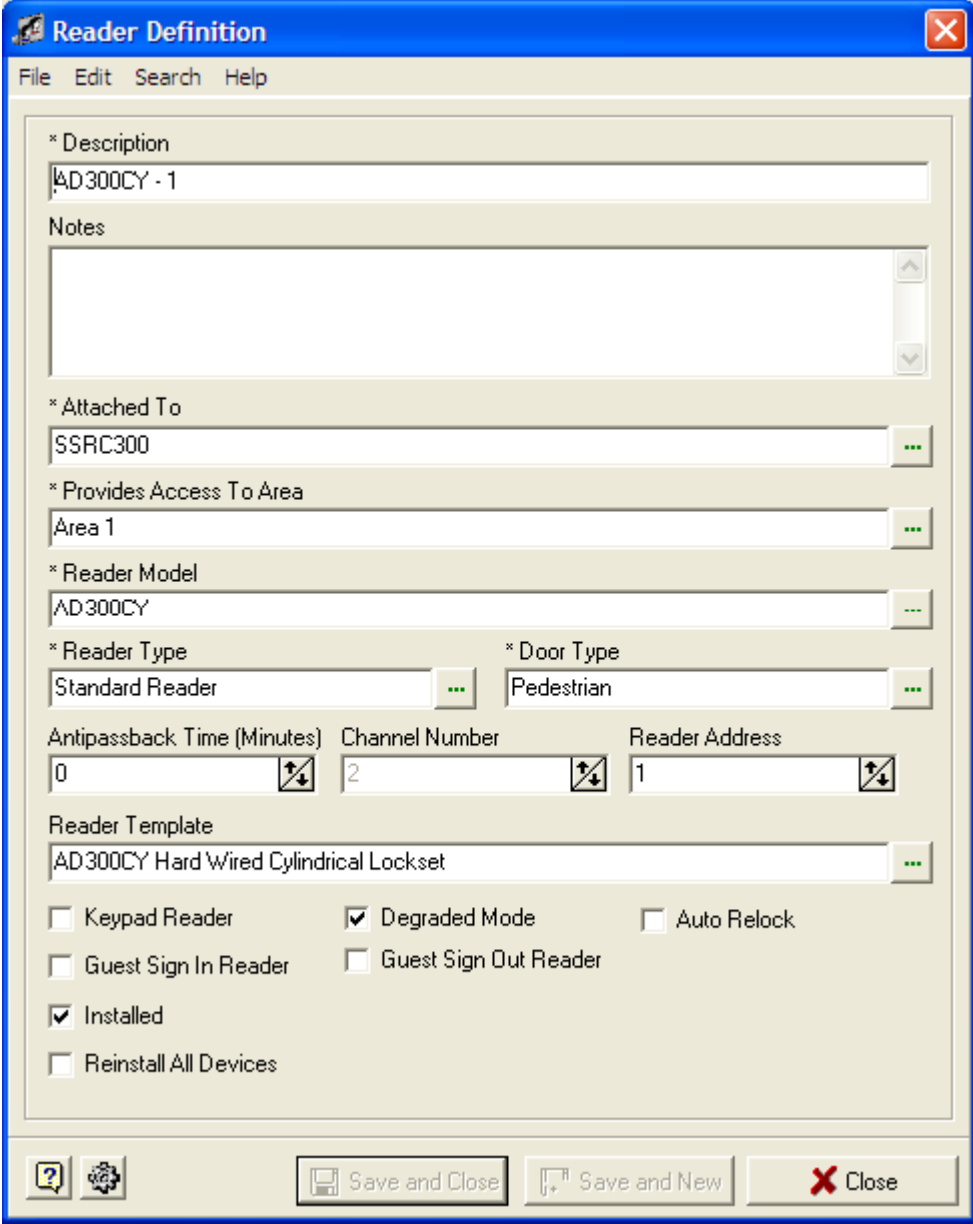
☒ Installed

☐ Reinstall All Devices

Help Save and Close Save and New Close

- 4 Add AD-300 locks and attach them to the SSRC-300 Controller. Remember that AD-300 readers will default to Channel 2 and the Reader Address will be one number more than defined with the SUS (Schlage Utility Software). **Example:** If the SUS defined the AD-300 lock as Address 0, then it would be defined as Address 1 in SMS. See the SMS Installation Manual for details.

Note: There are various templates the user can select depending on AD-300 model type. The templates will create all triggers, action items, AROs and MROs.



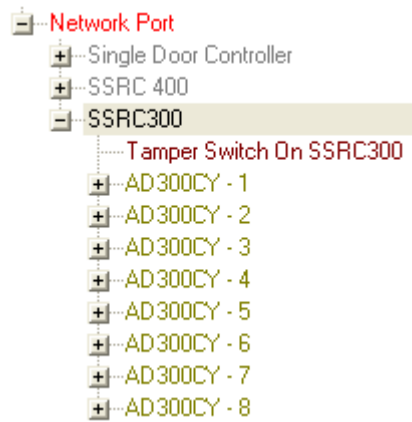
The image shows a 'Reader Definition' dialog box with a blue title bar and a menu bar containing 'File', 'Edit', 'Search', and 'Help'. The dialog is divided into several sections:

- * Description:** A text field containing 'AD300CY - 1'.
- Notes:** A large, empty text area with a vertical scrollbar.
- * Attached To:** A text field containing 'SSRC300' and a green ellipsis button.
- * Provides Access To Area:** A text field containing 'Area 1' and a green ellipsis button.
- * Reader Model:** A text field containing 'AD300CY' and a green ellipsis button.
- * Reader Type:** A text field containing 'Standard Reader' and a green ellipsis button.
- * Door Type:** A text field containing 'Pedestrian' and a green ellipsis button.
- Antipassback Time (Minutes):** A numeric field with a spinner, set to '0'.
- Channel Number:** A numeric field with a spinner, set to '2'.
- Reader Address:** A numeric field with a spinner, set to '1'.
- Reader Template:** A text field containing 'AD300CY Hard Wired Cylindrical Lockset' and a green ellipsis button.
- Checkboxes:**
 - ☐ Keypad Reader
 - ☒ Degraded Mode
 - ☐ Auto Relock
 - ☐ Guest Sign In Reader
 - ☐ Guest Sign Out Reader
 - ☒ Installed
 - ☐ Reinstall All Devices

At the bottom, there are three buttons: 'Save and Close' (with a floppy disk icon), 'Save and New' (with a floppy disk and plus icon), and 'Close' (with a red X icon). There are also help and settings icons on the left of the bottom bar.

- 5 Once defined, click on the **Save and Close** button.

Below is an example of the SSRC-300 Controller Definition if the template has been used:

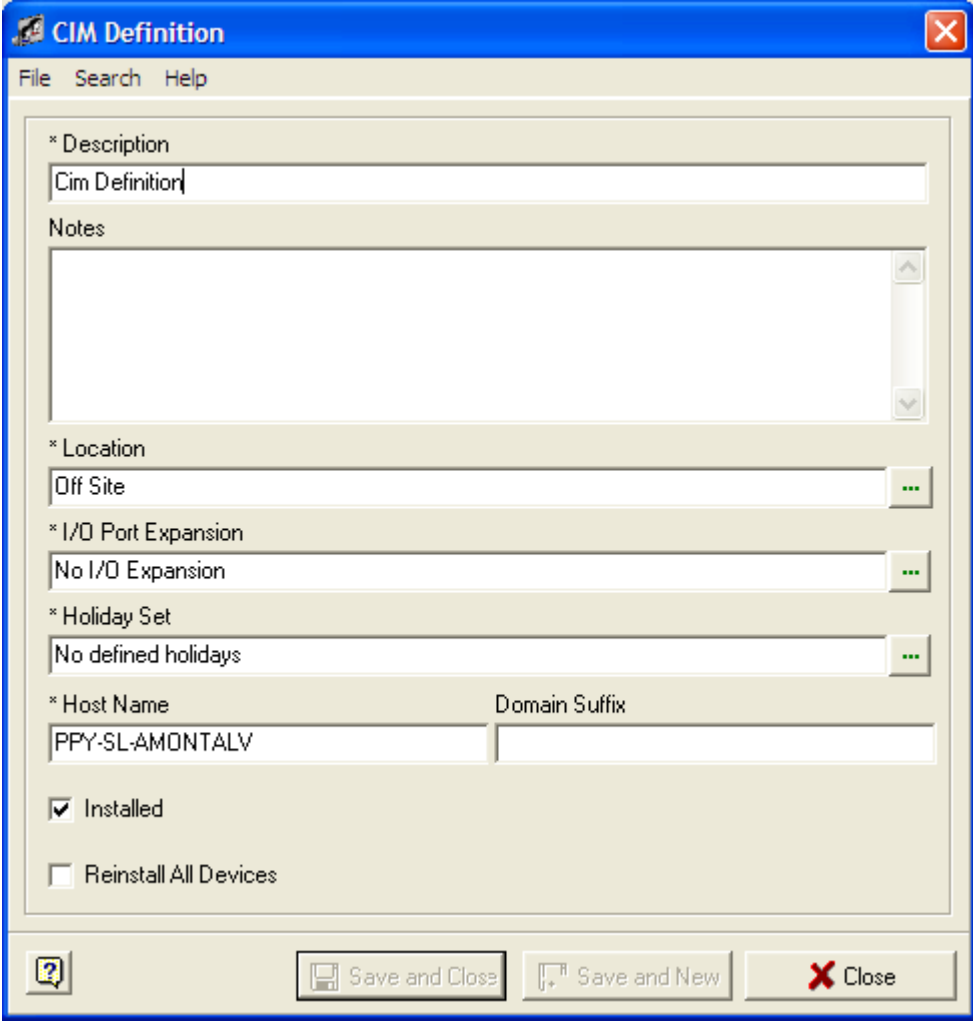


Define SSRC-400

The SSRC-400 is a variant of the SSRC. Instead of a single door controller, the SSRC-300 controls a single PIM400-485-SMS which can then communicate with up to 16 AD-400 Wireless locks.

To define an SSRC-400:

- 1 Set up your CIM Definition



The screenshot shows a Windows-style dialog box titled "CIM Definition". It has a menu bar with "File", "Search", and "Help". The main area contains several fields and checkboxes:

- * Description:** A text box containing "Cim Definition".
- Notes:** A large, empty text area with a vertical scrollbar.
- * Location:** A dropdown menu showing "Off Site" with a green ellipsis button to its right.
- * I/O Port Expansion:** A dropdown menu showing "No I/O Expansion" with a green ellipsis button to its right.
- * Holiday Set:** A dropdown menu showing "No defined holidays" with a green ellipsis button to its right.
- * Host Name:** A text box containing "PPY-SL-AMONTALV".
- Domain Suffix:** An empty text box.
- ☒ **Installed**
- ☐ **Reinstall All Devices**

At the bottom of the dialog, there is a toolbar with three buttons: a question mark icon, "Save and Close", and "Save and New" (with a plus icon). To the right of these is a "Close" button with a red X icon.

- 2 Define your CIM Port Definition

The screenshot shows a Windows-style dialog box titled "CIM Port Definition". It has a menu bar with "File", "Search", and "Help". The main area contains several fields and checkboxes:

- * Description: A text box containing "Network Port".
- Notes: A large empty text area with a vertical scrollbar.
- * Attached to CIM: A dropdown menu showing "Cim Definition" with a green ellipsis button to its right.
- * Com Port: A dropdown menu showing "Network" with a green ellipsis button to its right.
- * Baud Rate: A dropdown menu showing "N/A".
- ☐ Modem Attached
- ☒ Installed
- ☐ Reinstall All Devices

At the bottom, there is a toolbar with three buttons: a question mark icon, "Save and Close" (with a floppy disk icon), and "Save and New" (with a floppy disk and plus icon). To the right of these is a "Close" button with a red X icon.

- 3 Add your SSRC-400 controller and attach to the CIM port definition. Use the new controller model: SSRC-400.

Note: Make sure the SSRC has been configured on the network prior to entering the values here. See the installation manual for details.

Controller Definition

File Search Help

* Description
SSRC 400

Notes

* Attached To I/O Port or Master
Network Port ...

Location
Off Site ...

* Controller Model
SSRC-400 ...

Callback Set
No callback numbers ...

Site Code Set
No defined site codes ...

Holiday Set
No defined holidays ...

* Locale Timezone
(GMT-05:00) Eastern Time (US & Canada) ...

IP Address or Host Name
10.45.49.65

IP Port Number
3001 ...

Encrypted ☐

Phone Number

Master Channel
N/A

Board Address
N/A

Schedule Timezone
Never

Network Device Type
Schlage SIPRCNX ...

Administrative Level Password

Access Level Password

Domain Suffix

☒ Installed

☐ Reinstall All Devices

Save and Close Save and New Close

- 4 Add the PIM400-485-SMS controller and attach it to the SSRC-400 controller. The channel of the PIM400 will default to 2 and cannot be altered. The address of the PIM400 will be one higher than what was defined in the Schlage Utility Software (SUS). **Example:** If the SUS defined the PIM400 as Address 0, then it would be defined as Address 1 in SMS. See the SMS Installation Manual for details.

Controller Definition

File Search Help

* Description
SSRC400 PIM400

Notes

* Attached To I/O Port or Master
SSRC 400

Location
Off Site

* Controller Model
PIM400-485-SMS

Callback Set
No callback numbers

Site Code Set
No defined site codes

Holiday Set
No defined holidays

* Locale Timezone
(GMT-05:00) Eastern Time (US & Canada)

IP Address or Host Name

IP Port Number
3001

Encrypted

Phone Number

Master Channel
2

Board Address
1

Schedule Timezone
Never

Network Device Type

Administrative Level Password

Access Level Password

Domain Suffix

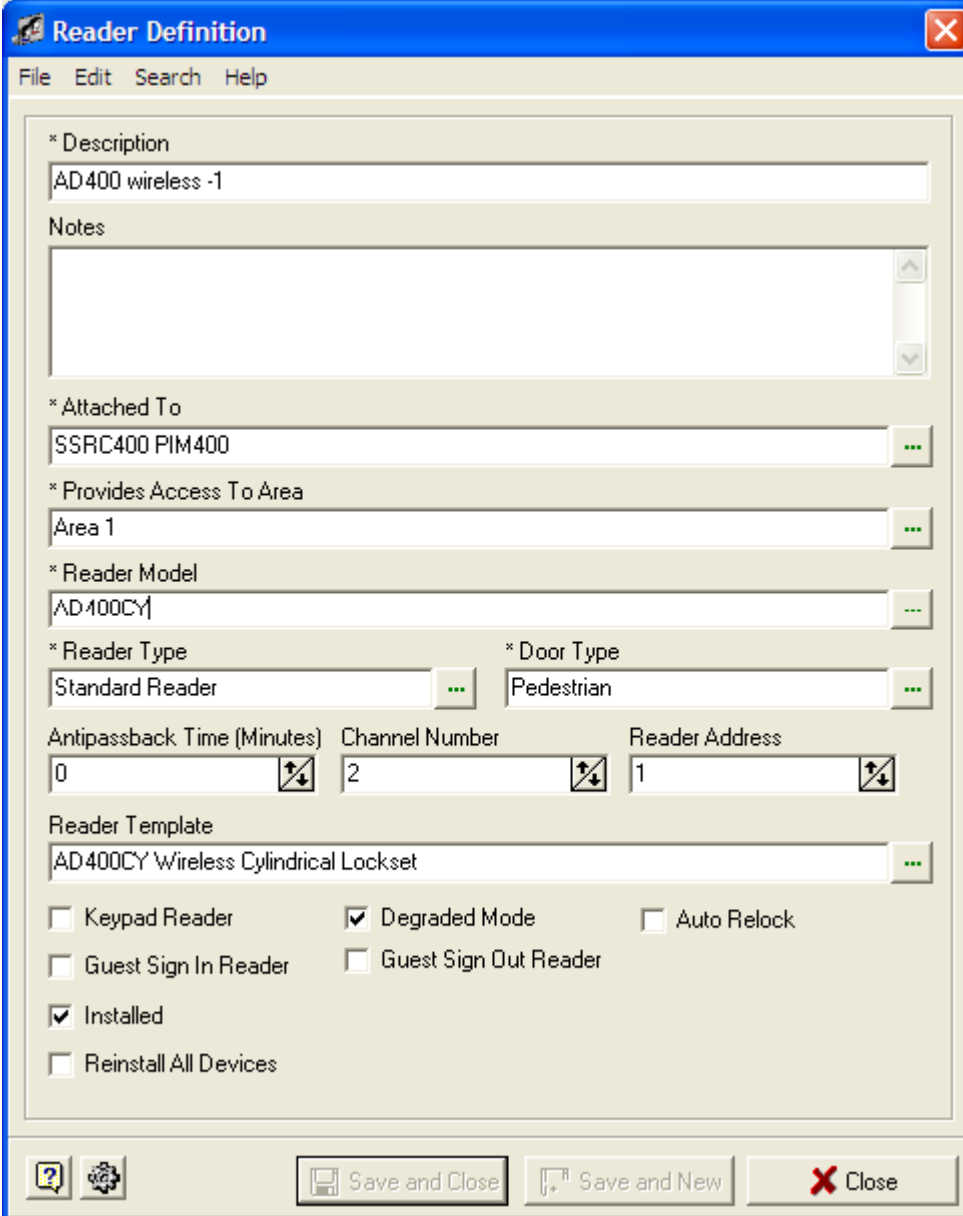
☒ Installed

☐ Reinstall All Devices

Save and Close Save and New Close

- 5 Add AD-400 locks and attach them to the PIM400-485-SMS. Any AD-400 lock that is attached to the PIM400 will use channel address 2.

Note: There are various templates the user can select depending on AD-400 model type. The templates will create all triggers, action items, AROs and MROs.



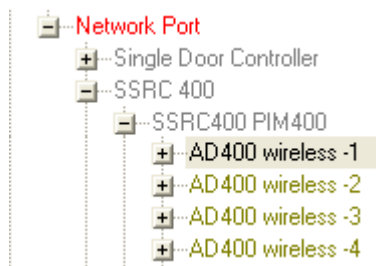
The image shows a 'Reader Definition' dialog box with a blue title bar and a menu bar containing 'File', 'Edit', 'Search', and 'Help'. The dialog is divided into several sections:

- * Description:** A text field containing 'AD400 wireless -1'.
- Notes:** A large, empty text area with a vertical scrollbar.
- * Attached To:** A text field containing 'SSRC400 PIM400' and a green ellipsis button.
- * Provides Access To Area:** A text field containing 'Area 1' and a green ellipsis button.
- * Reader Model:** A text field containing 'AD400CY' and a green ellipsis button.
- * Reader Type:** A text field containing 'Standard Reader' and a green ellipsis button.
- * Door Type:** A text field containing 'Pedestrian' and a green ellipsis button.
- Antipassback Time (Minutes):** A numeric field with a spinner, set to '0'.
- Channel Number:** A numeric field with a spinner, set to '2'.
- Reader Address:** A numeric field with a spinner, set to '1'.
- Reader Template:** A text field containing 'AD400CY Wireless Cylindrical Lockset' and a green ellipsis button.
- Checkboxes:**
 - ☐ Keypad Reader
 - ☒ Degraded Mode
 - ☐ Auto Relock
 - ☐ Guest Sign In Reader
 - ☐ Guest Sign Out Reader
 - ☒ Installed
 - ☐ Reinstall All Devices

At the bottom, there are three buttons: 'Save and Close' (with a floppy disk icon), 'Save and New' (with a floppy disk and plus icon), and 'Close' (with a red X icon). There are also help and settings icons on the left.

- 6 Once defined, click on the **Save and Close** or **Save and New** button.

Below is an example of the SSRC-400 Controller Definition if the template has been used:

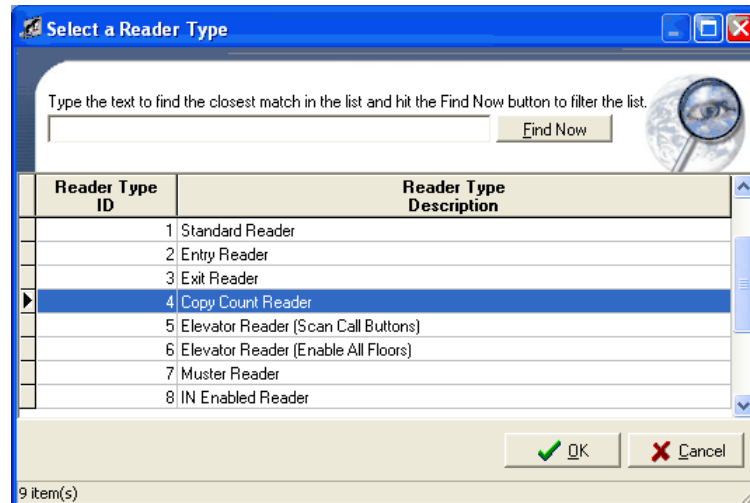


Define a Reader

- 1 To define a reader click on the **Edit Readers** tab in the Options section and the **Edit Readers** tab in the Information Grid becomes active. Click on the + sign.
- 2 The **Reader Definition** window opens. For a basic reader you must program a reader and a relay. If you are going to use a contact point of the reader interface then you must program one of them also.

- 3 Enter a description and the notes relevant to it.
- 4 Next, select the controller that the reader is attached.

- 5 Select the area that the reader is providing access. Click on the expand button to open the **Select an Area** window. Highlight the area and click **OK**.
- 6 Select the reader model. If you are defining a VIP reader, to let the controller know that the device is a VIP reader, you should select the Model to be the Schlage VIP Lock.
- 7 Select the reader type. The system provides seven (7) factory set reader types. Additional reader types can be defined using **Reader Type Definition** window. **Edit>Reader Types**.



In Enabled Reader - This reader is used to stop people from tailgating. If the user does not swipe the card at the entry reader, that person will not be given access to any area in the building that is secured by the In Enabled Reader.

Antipassback Reset Reader - Swiping the card at this reader resets the card to neutral.

Muster Reader - This reader is used for creating evacuation reports.

- 8 Select the door type through which the reader is giving access.
- 9 Enter the Antipassback time. See the section below for further information about Antipassback.

Antipass Back

Antipassback is a function that prevents cardholders from passing their card to another person for illegal entry. The same card cannot be used at an entry or exit reader twice in a row. In other words, once a card is presented at an entry reader, it must then be presented at an exit reader. If a card is presented twice in a row at the same type of reader, no access will be granted. The Transaction Monitor will display an anti pass back violation transaction. It is commonly used at car park barriers and turnstiles.

Antipassback Time - This is the time in minutes that your system will reset the cardholder's Antipassback state to neutral. For example, if a card is swiped at an entry reader and anti pass back time is set to 10 minutes, then after 10 minutes that card will be reset and access will be granted at an entry reader again even though the cardholder has not used an exit reader.

Global Anti pass back - Global anti pass back is used with a parent/child setup and participating Entry and Exit readers attached to these boards. It works with SRCNX Firmware V5.50 and higher. Every controller board in the parent/child set up that has entry or exit readers attached must have dip switch 5 open. When a valid entry occurs, the cardholder is registered as "In" and a message is sent to the parent controller board. The parent board then forwards the message to all its child boards to update this person's Antipassback state.

Local Antipassback - The local Antipassback option must be used if the cardholders need to gain access more than one entry reader before presenting at an exit reader that is on a parent-child configuration.

- 1 Enter the channel number in the controller to which this reader is attached.
- 2 Enter the channel address.
- 3 Select the reader template. (See the section below for further information).

Reader Template

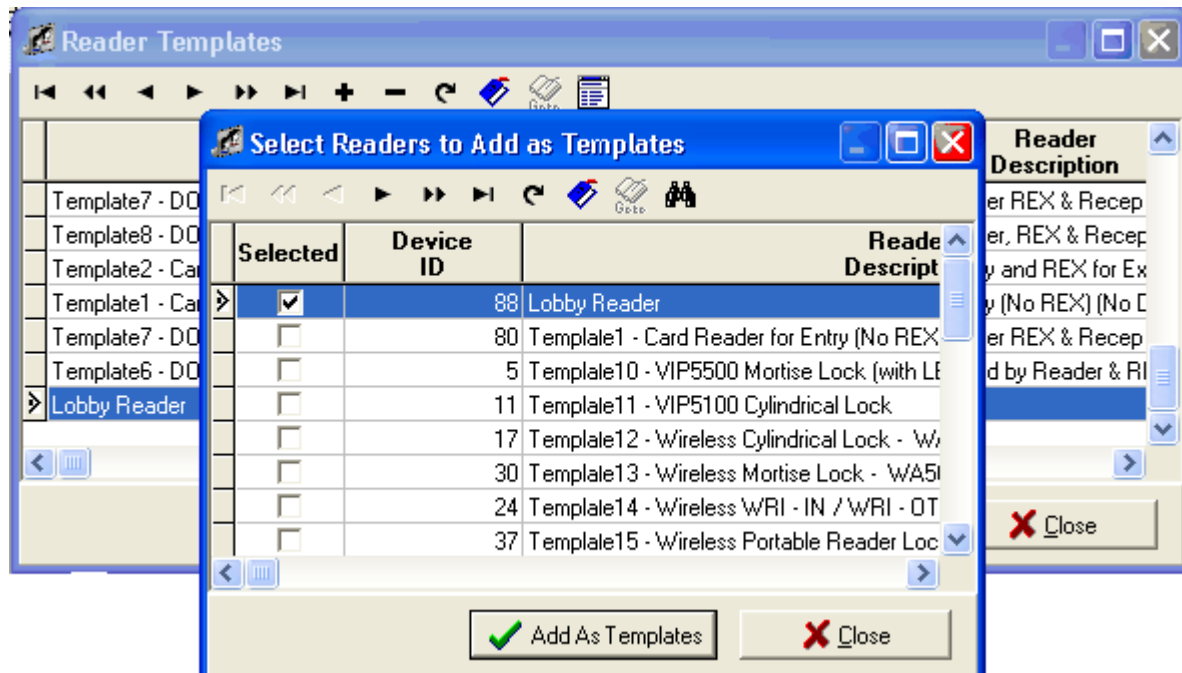
Readers are designated as templates when you have additional readers that use the same or very similar relay, contact, event trigger and override information. A template duplicates the information so that it does not have to be redefined each time a new reader is added to the database. For instance, a reader template is used if you have 16 readers attached to one controller board and they use related programming. Once you have programmed the first reader, it can be defined as a reader template. After a template is assigned to a new reader, the **Template Choices** window offers to duplicate other features of the Reader Template. Verify that all contacts, relays, event triggers and overrides have been previously defined before assigning a reader template.

Defining a Reader as a Template

Follow these steps to define a reader as a template:

1. Define a reader you want to set as a template.
2. Go to System Manager main window, select **Edit>Reader Templates**.

- The **Reader Templates Definition** window opens. Click on the Add Readers as Templates (+) button. This opens the **Select Readers to add as Templates** window.



- Choose the reader you want to set as template by clicking on the checkbox. Now click the **Add as Templates** button. The selected reader appears in the reader templates list. If you want to edit the definition, either double click on the record you want to edit or select the reader template and click on the **Edit current record** button from the toolbar.

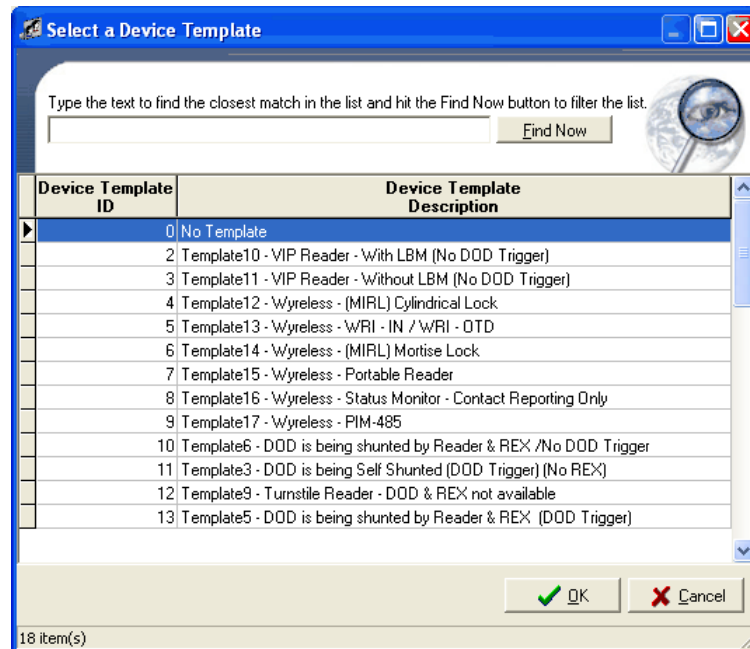
Factory set templates are available for Wireless, VIP, and standard readers. Contacts, relays, event triggers, and manual overrides are predestined. More information on each template is available on the **Reader Definition>Notes** field. Go to **System Manager>Edit Readers**. Select a reader template from the grid view. Double click on the record to open it. The Notes field displays details about the reader. The system allows you to modify any information that is attached to these templates. When you try to delete a factory set template, you are prompted with a Warning message to confirm the action.

The screenshot shows the 'Reader Definition' dialog box with the following fields and options:

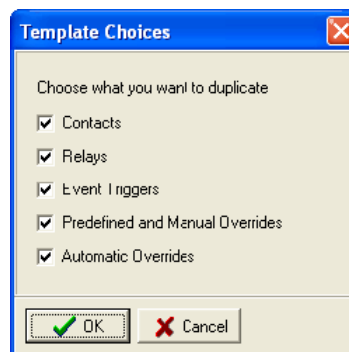
- * Description:** Template10 - VIP5500 Mortise Lock (with LBM)
- Notes:** VIP Lock allows entry into this door. Lock Handle Exit Request (REX) allows exiting thru the door. Door Status Contact (DOD) is available for monitoring. Reader & Exit Request will shunt DOD. Key Switch Monitor & LBM available. No Trigger on (DOD).
- * Attached To:** Template / SRCNX - VIP Controller
- * Provides Access To Area:** Off Site
- * Reader Model:** Schlage VIP Lock
- * Reader Type:** Standard Reader
- * Door Type:** Pedestrian
- Antipassback Time (Minutes):** 0
- Channel Number:** 1
- Reader Address:** 1
- Reader Template:** No Template
- ☐ Keypad Reader
- ☒ Degraded Mode
- ☐ Auto Relock
- ☐ Guest Sign In Reader
- ☐ Guest Sign Out Reader
- ☐ Installed
- ☐ Reinstall All Devices

At the bottom, there are icons for help, a refresh button, and three buttons: 'Save and Close', 'Save and New', and 'Close'.

Highlight and select a template and click **OK**. If the templates available here do not match your specific requirements, select No Template and click **OK**. In this case you need to manually program the contacts, relays, event triggers and overrides for this reader.



If you select a template, the **Template Choices** window displays prompting you to choose the information you want to duplicate while using the selected template. Make your selection by clicking the check box and choose **OK**.



- 1 Select the **Keypad Reader** check box if this is a keypad reader.
- 2 Select **Degraded Mode** check box if you are going to use this functionality. See the section below.

Degraded Mode

Degraded Mode is an operating state for the Reader Interface (RI) which, when set, allows access by evaluating just the site codes. The reader enters degraded mode if the operator has enabled degraded mode and the reader interface has lost communication with the SRCNX.

In this situation, the SRINX notices the card presentation and realizing that it has no communication with the SRCNX, checks to see if the badge has proper site codes. It energizes the relay if the site code matches. When using Degraded Mode, an alarm for "Lost link to Reader" should be programmed to alert alarm workstations that communication between the board and reader interface has been interrupted.

- 1 Select the **Guest Sign In Reader** checkbox if this reader is assigned for automatically signing in the guests in the Guest Pass System* application.
- 2 Select the **Guest Sign Out Reader** checkbox if this reader is assigned for automatically signing out guests in the Guest Pass System* application.
- 3 **Auto Relock** - This option resets the triggers (contacts and relays) on a particular event and relocks the door.
- 4 Select the **Installed** check box to install this reader in the system.

Note: Deselecting the Installed check box uninstalls all the devices attached to this reader.

- 5 If you deselect the **Installed** check box, the reader and the associated devices are uninstalled. Then the **Reinstall all Devices** checkbox becomes active. Select this option to reinstall all the devices in the system.

Contact Definitions

- 1 Click on the **Edit Contacts** tab in the options bar. The Edit Contacts tab in the Information Grid becomes active. Click on the + sign to define a new contact. The Contact definition window opens.

- a) Enter a description for the contact and the notes attached with it. Make sure that you describe what kind of a contact you are defining. E.g. REX (Reader Exit Request), DOD etc.

- b) Next select the reader or controller based on where this contact is attached.
- c) Select the location (Area) for this contact.
- d) Select the contact type.

REX (Reader Exit Request) - REX is a contact type that has a "Normally Open" state. It is recommended that REX be used as Input 1 when adding contacts to the database.

DOD (Door Open Detect) DOD is a Contact Type whose state is "Normally Closed." It is recommended that a DOD be used as Input 2 when adding contacts to the database.

- e) The **Associated Elevator Reader** selector is disabled. It will become enabled for contact definition if the contact type is an elevator call button.
- f) **Alarm Samples** - The SRCNX board will sample contact points by measuring voltage on the line. It measures the voltage on each point, one after the other. Alarm Samples are the number of consecutive measurements that must be made before deciding that the state has changed from secure to alarm or alarm to secure.
- g) **Fault Samples** - This is the number of samples to be done between reporting trouble/ open short and contact secure. The fault sample is usually a higher number to ensure against measurements taken at the moment that a point is either opening or closing.
- h) **Parallel Resistor** - Enter the number of Ohms of the Parallel Resistor in this field. A single resistor in parallel with the contact should be used when the contact point is normally open.
- i) **Series Resistor** - Enter the number of Ohms of the Series Resistor in this field. A single resistor in series with the contact should be used when the contact point is normally closed.
- j) **Debounce Period** - This is the period of time that must elapse before reporting a second alarm on the same point. The debounce period is used to inhibit the reporting of alarms over and over. For example, the debounce period is set to 10 seconds. A person walks down the hallway. The motion detector is triggered and Contact Active is reported. The point returns to secure and then active again, etc. At the end of 10 seconds, the state of the contact is reviewed. If the contact is still active, nothing more is reported until the contact is secured.
- k) **Input Number** - This is the contact number on the Reader Interface. Specify the contact point that is used for this contact.
- l) **Verify Status** - This checks the status of the door and sends a signal to the contact point once the door comes out of the automatic override state. For example if the automatic override time ends at 5.00 PM and the door is still open, the system gets a Door Held Open alarm.
- m) **Normally Open** - If this option is checked "Normally Open" be the normal state of the contact point. The contact reports alarms if the contact is in the "Normally Closed" state.

Contact Point Supervision using Parallel and Series Resistors

Contact points are supervised to detect any tampering with the equipment, including breaks and/or shorts in the cable between the reader controller and the supervised input point. Resistors allow the controller to distinguish between a contact opening and closing compared to a circuit opening or shorting.

Note: Please refer to **Schlage Hardware Manual** for more information on Contact Point Supervision.

Parallel and Series resistors are used with contact point supervision.

Define a Relay

- 1 To define a relay, click on the **Edit Relay** tab in the Options View section. The **Relay Definition** window will open. Enter the required information. Note that the **Associated Elevator Reader** selector is disabled. It will become enabled for relay definition if the relay type is an *Elevator Floor Select*.

- a) **Description** -Type in the name of the respective relay you are configuring,
- b) **Notes** - If necessary, write any pertinent information about this relay.
- c) **Attached to Which Controller or Reader** - Define the controller or reader to which the relay is attached.
- d) **Location** - Define the location of the relay.
- e) **Relay Type** - Select the type of the relay. If this relay is used for an elevator, change this to *Elevator Floor Select*. The system provides eleven factory set relay types. The relay types can be added, modified or deleted using **Edit>Relay type**.
- f) **Relay Number** - Enter the number of the respective relay.

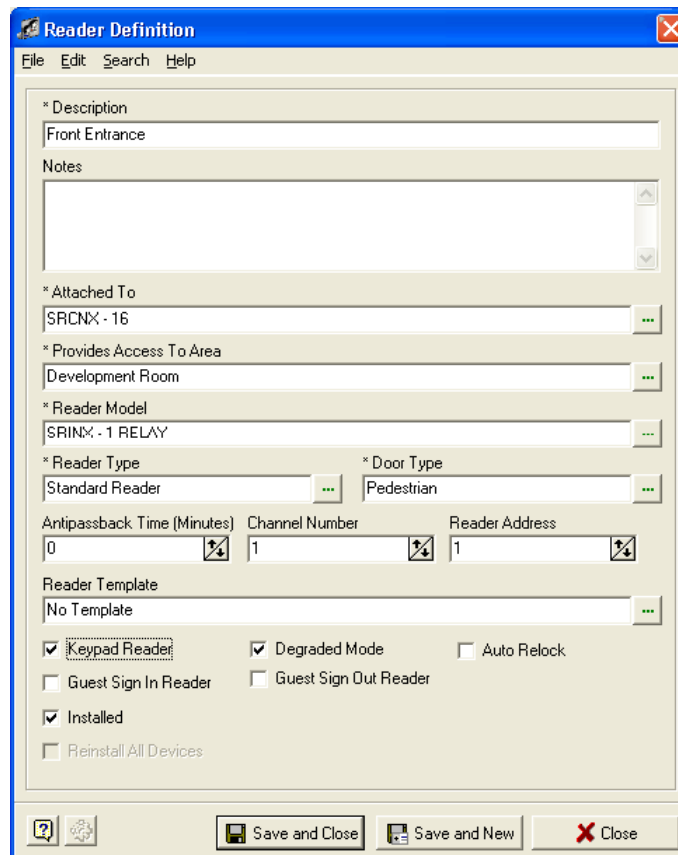
Access Under Duress Transactions

Access Under Duress is a feature by which a person entering an area under threat may signal an alarm at the console by entering a PIN number which is exactly one greater than his/her assigned PIN number (keypad ID). For example, if the PIN number is 1234, entering 1235 will generate an "Access Under Duress" transaction as opposed to a "Valid Access" transaction. The firmware must be modified to support this option.

At the moment, we only expect to support this feature with the SRCNX and SRINX boards. These are the points to be noted while defining an access under duress transaction.

- 1 Define a keypad reader.
- 2 Select the reader type as **Standard Reader**.

- 3 Check the box near the option **Keypad Reader**.

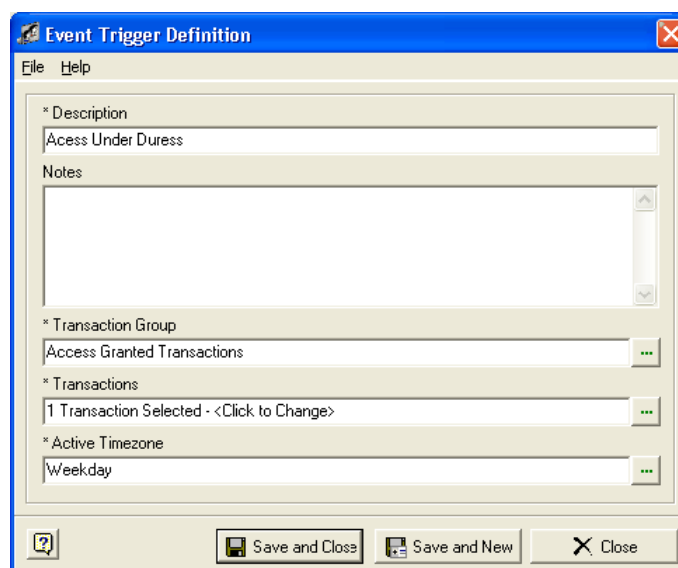


The **Reader Definition** dialog box is shown with the following fields and options:

- Description:** Front Entrance
- Notes:** (Empty text area)
- Attached To:** SRCNX - 16
- Provides Access To Area:** Development Room
- Reader Model:** SRINX - 1 RELAY
- Reader Type:** Standard Reader
- Door Type:** Pedestrian
- Antipassback Time (Minutes):** 0
- Channel Number:** 1
- Reader Address:** 1
- Reader Template:** No Template
- ☒ **Keypad Reader**
- ☒ **Degraded Mode**
- ☐ **Auto Relock**
- ☐ **Guest Sign In Reader**
- ☐ **Guest Sign Out Reader**
- ☒ **Installed**
- ☐ **Reinstall All Devices**

Buttons at the bottom: **Save and Close**, **Save and New**, **Close**.

- 4 Define the event trigger for the reader.

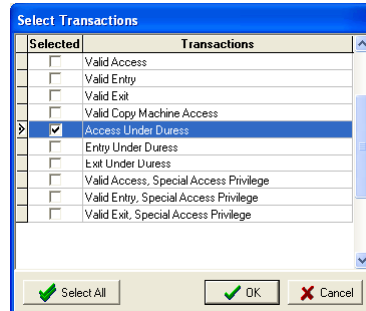


The **Event Trigger Definition** dialog box is shown with the following fields and options:

- Description:** Access Under Duress
- Notes:** (Empty text area)
- Transaction Group:** Access Granted Transactions
- Transactions:** 1 Transaction Selected - <Click to Change>
- Active Timezone:** Weekday

Buttons at the bottom: **Save and Close**, **Save and New**, **Close**.

- 5 Select **Access Granted Transactions** as the transaction group.
- 6 Next select **Access Under Duress** as the **Transaction**.



How to Alarm an Access Under Duress Transactions

If you present your card and enter your assigned pin number on the keypad, you will get an access granted transaction. To get an access under duress transaction you should add 1 to your pin number. For example if your pin number is 6425 you should press 6426 to get access under duress. If the pin number is 2999 you should enter 3000 to get an access under duress transaction.

Entry and Exit Under Duress

In the similar way you can define Entry Under Duress and Exit Under Duress transactions. The reader type that is used to define these transactions should be entry or exit readers. You should also choose appropriate transactions (Entry Under Duress and Exit Under Duress) while defining the event triggers. The user can signal these alarms by entering one number greater than their assigned pin numbers.

Event Triggers

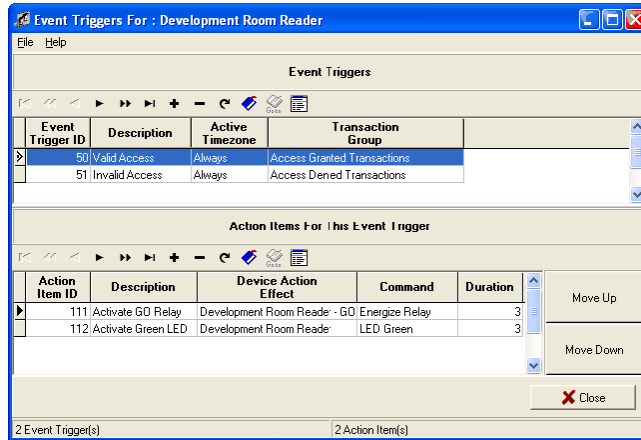
Once you have entered all your information for your readers, contacts, and relays, an event trigger must be assigned. An **Event Trigger** is a transaction that must have an action, a command and a device associated with it.

Triggers are critical because they determine what will happen when an event (or transaction) occurs. For example, a cardholder presents a card at a reader and expects to be granted access to an area. Presenting the card is a transaction. However, specific actions must be defined to send commands to a device or devices to allow the door to open.

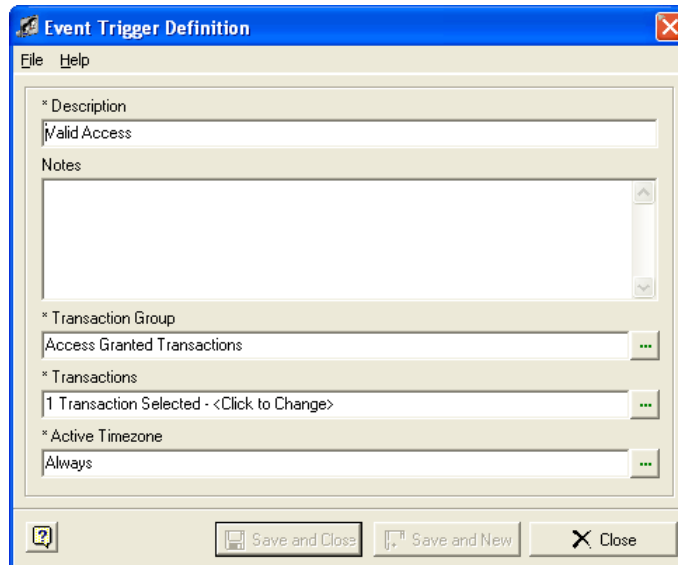
Event Triggers are made up of two parts, the Event Trigger and the Action Items for the Event Trigger. Triggers need to be programmed for every function that you want that device to do.

- 1 The **Trigger Action Order** in the examples that follow is not the only order that should be followed. Your specific device functionality determines the order of the Trigger Actions. To program the Triggers, go to the **Hardware Map** section and select the device that you want the trigger for, then select **Edit>Edit Event Triggers**. In this case we would locate *Main Lobby Reader- New York* and open the definition and then click on the gear icon.

- 2 The **Event Trigger for Main Lobby Reader** window opens.

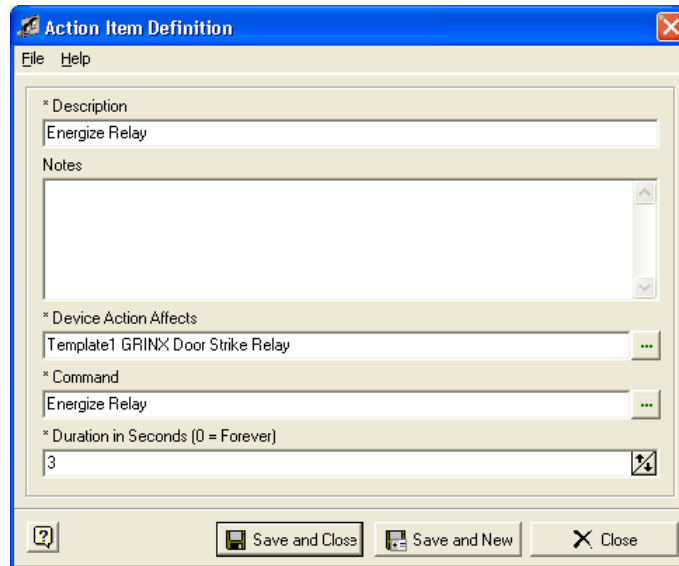


- 3 First we will define the event trigger for this reader. Click on the + sign on the upper part of the window. The **Event Trigger Definition** window opens.



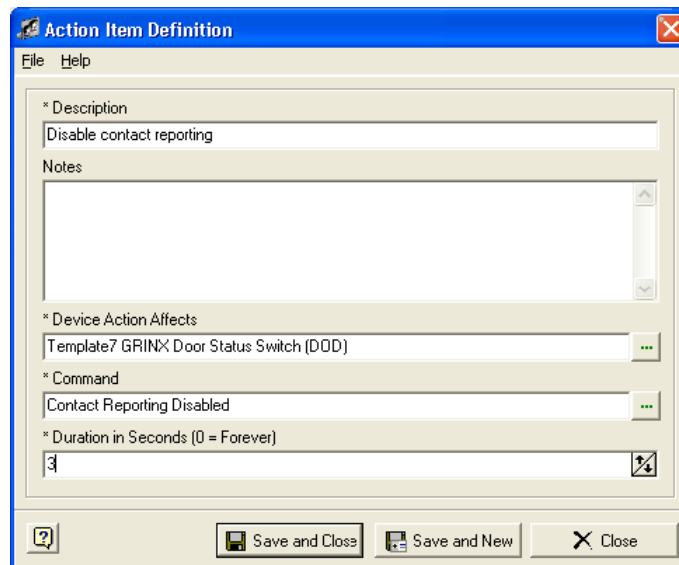
- 4 Enter a Description, notes and select a **Transaction Group**, which will be Access Granted Transactions.
- 5 The **Transaction Group** will in turn determine the type of transactions that are offered. Click on the expand button to select a transaction group.
- 6 Click on the expand button to select a transaction.
- 7 Select the time zone you want the trigger to function in by clicking on the expand button. Click **Save and Close**.
- 8 Click **OK** to return to the main Event Trigger screen.
- 9 Now we will program **Actions** that are associated with the transaction. In the Actions Item section of the Event Trigger main window, click on the + sign. Enter your Description.

- 10 To select the specific device that this action is going to effect, click on the expand button near the **Device Action Affects** field. Click on the expand button and select a device. Click **OK**.
- 11 Next, click on the expand button near the **Command** field to select a command for the device. For this example, we will choose **Energize Relay**. The duration setting sets the amount of seconds the relay will be energized. In this example the duration is set for 3 seconds, if zero (0) is entered then the relay will be energized forever, which means the relay will be always energized.



The screenshot shows the "Action Item Definition" dialog box. It has a menu bar with "File" and "Help". The "Description" field contains "Energize Relay". Below it is a "Notes" text area. The "Device Action Affects" field shows "Template1 GRINX Door Strike Relay" with an expand button (three dots). The "Command" field shows "Energize Relay" with an expand button. The "Duration in Seconds (0 = Forever)" field contains the number "3" and has a small icon to its right. At the bottom are buttons for "?", "Save and Close", "Save and New", and "Close".

- 12 The next **Action Command** that needs to program is the command to turn the **LED Green**. Program the **Duration Setting** for three seconds to synchronize it with the Energize Relay setting.
- 13 If we are using a contact input off of the reader, then we have to program actions for that DOD contact. Select the contact that is going to be the DOD.



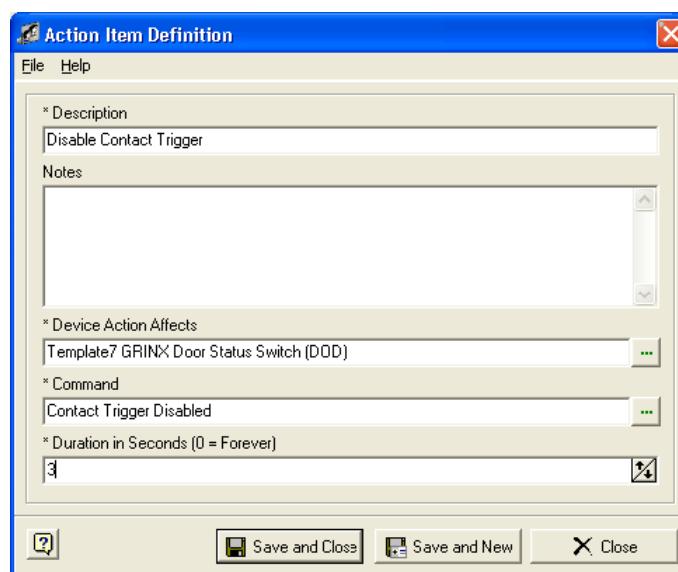
The screenshot shows the "Action Item Definition" dialog box. It has a menu bar with "File" and "Help". The "Description" field contains "Disable contact reporting". Below it is a "Notes" text area. The "Device Action Affects" field shows "Template7 GRINX Door Status Switch (DOD)" with an expand button (three dots). The "Command" field shows "Contact Reporting Disabled" with an expand button. The "Duration in Seconds (0 = Forever)" field contains the number "3" and has a small icon to its right. At the bottom are buttons for "?", "Save and Close", "Save and New", and "Close".

There are two Commands that have to be programmed for the DOD Contact. The first is **Contact Reporting Disabled**. This prevents the **Contact Active** transaction, which may be an Alarm, from being sent for the amount of time that is set in the **Duration of Seconds** field. Again set the Duration time for 10 seconds.

- 14 The second Action Item Command is **Contact Trigger Disabled**. This command prevents any device that is attached to that contact, such as a bell above a door, from being enabled for the amount of the Duration Time.

The **Duration Time** is set at 10 seconds, the same as the Contact Reporting Disabled Action that was done previously.

The completed Access Granted Trigger for the Front Door proximity reader should look like the one below.



The examples up to this point have shown how to program Event Triggers/Actions step by step.

Define CM Locks

The **Schlage SMS** allows the user to create offline reader devices (locks) within hardware definitions. The offline readers do not directly communicate with the host controller. So it is necessary to do manual programming at the reader location. The user can create necessary downloadable files and upload to a pocket PC. The data is transferred to a PDA by connecting to the serial communication port of the PC or via a USB port for the AD-200 Series. The files required for programming the locks are generated to a folder using the **Offline Lock Interface Module**. The programming of doors is accomplished by connecting a **CIP** (Computer Interface PAK) from the laptop/palmtop to the iButton ports of the lock or to the USB port of the lock for AD-200 Series.

Follow these instructions to define a CM lock:

Note: The user needs at least read only permissions to the System Manager item for offline locks to see the offline locks defined in the system.

- 1 In the option bar, select **Hardware Map>CM Locks**.

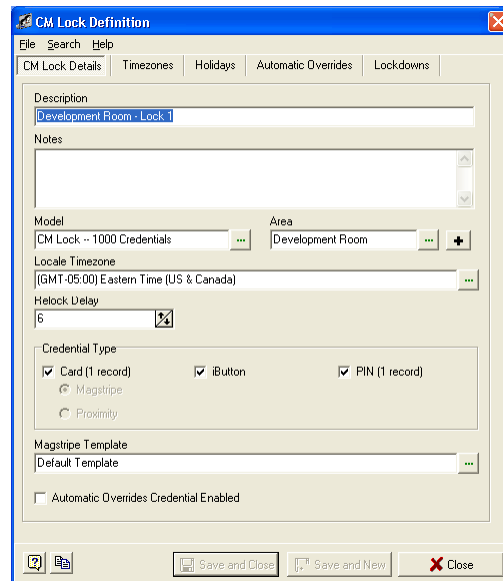
- 2 In the Grid window **Offline Locks** tab is activated. Click the + sign (insert button). The **CM Lock Definition** window opens. This dialog allows the user to define new locks, and modify existing definitions.

- 3 The window defaults to **CM Lock Details** tab.
- a) **Description** - Enter a description for the offline lock you are defining.
 - b) **Notes** - Enter notes associated with it.
 - c) **Model** - Click the browse button to select the model of the lock. On the **Select a Model** window, choose the correct model by highlighting it and click **OK**.
 - d) **Area** - Select the area the lock is providing access to by clicking the expand button. You can create a new area by clicking on the plus button (+). On the **Create Area Definition** window, enter a description. Area Type, Maximum Occupancy Count and Area State fields displays factory set information.

Note: Assigning an area is for organization and security purposes only, and is not used for assigning access privileges to the lock. Giving a cardholder access to an area does not give him/her access to offline locks. In the **System Security** program, When permissions to the **All Areas** Area Set under Area Set permissions is set to Read Only or None, the Add Area button on this window is disabled.

- e) **Locale Timezone** - Click the browse button to select a locale timezone.
- f) **Relock Delay** - Specify the number of seconds required to relock the lock.
- g) **Card Types** - Select the technology supported by the lock. You need to select at least one of the available technologies (Card, iButton or PIN). If you select the option Card, the radio buttons for **Magstripe** and **Proximity** credentials are enabled. Select the credential technology that you are going to use for this particular lock. It is very important to select the appropriate technology, because you cannot mix Magstripe and Proximity credentials on one lock. So, while adding access records for this lock, the system allows you to add only those credentials with the technology you have specified here for the lock.

Once a credential has been added to the lock, both the Proximity and Magstripe radio buttons are inactive. This prevents modification of the Lock credential technology type after a credential is attached. In order to modify the credential technology after a credential has been added, the credential has to be removed first.



- h) **Magstripe Template** - Each lock can use its own Magstripe template. Click on the browse button to select a template. If the user changes a template that is already in use, the CM Lock credentials that are entered manually will be affected. This field defaults to Default Template. Also note that if you have selected Proximity as the credential type, the Magstripe Template field is disabled.

Note: For further information on Magstripe Template, refer to the **Magstripe Template Definition** section in this chapter.

- i) **Automatic Overrides Credential Enabled** - If this option is selected, the automatic override will be enabled only with a valid card swipe. For example, if a door is scheduled to open at 8 AM, that door will not unlock until there is a valid access transaction. This feature is useful at the event of unknown factors like heavy snow etc. and the door need not be opened at the scheduled time.

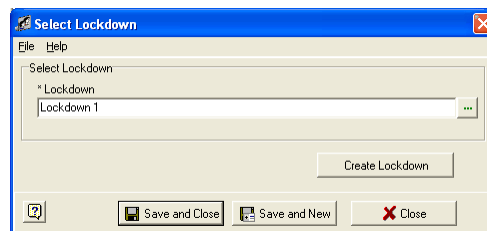
Note: If the dialog is in edit mode when the user attempts to uncheck a technology that is supported by the lock (Card, iButton, or PIN) and the lock currently has credentials attached to it with the technology, the user will get an error message and will not be able to uncheck the box. The user must remove all of those credentials from the lock before modifying the information. There is a number next to the checkbox that lists the number of credentials attached to the lock that uses this technology.

- 4 Next, you need to attach time zones to this lock. You can attach a maximum of sixteen (16) time zones per lock. Select the **Timezones** tab on the **CM Lock Definition** window.
- a) Select the + sign to add time zones. All the time zones (with single intervals) defined in the system are displayed. Use the Search feature to easily locate time zones. The user can select and add multiple time zones at the same time. Click **OK**.

Note: While defining Offline Lock Access, if you select a timezone that is not attached to the lock, the lock will not be available for granting access.

- 5 Now you need to attach holidays to the offline lock. You can attach up to thirty two (32) holidays per lock. Select the **Holidays** tab on the **CM Lock Definition** window.

- a) Select the + sign to add holidays. All the holidays defined in the system are displayed. Use the Search feature to easily locate holidays. The user can select and add multiple holidays at the same time. Click **OK**.
 - b) Select an offline function to apply to the lock.
 - **Passage** - The offline device will allow access during the specified holiday.
 - **Secured** - The offline device will be locked and will not allow access through the door during the specified holiday.
 - **Secured Lock Out** - The lock will not allow access, but will allow people with special credential to go through the door during the specified holiday.
 - 6 Now add the **Automatic Overrides** to the lock. Clicking the + sign opens the **Automatic Override Definition** window. Define the override and attach the timezone during which you want to unlock and lock the door. The system allows you to attach a timezone with multiple intervals to an ARO, only if the timezone interval is a spanning midnight timezone. A maximum of eight (8) automatic overrides and lockdowns are allowed per lock. Once the total number of lockdowns and automatic overrides reaches the maximum number (8), a new record can be added, but the user will have to replace it with an existing lockdown or automatic override.
-
- Note:** CM locks do not allow the attachment of multiple AROs with same time schedule. The system also does not permit AROs with overlapping time schedule attach to CM Locks. E.g. If there is a timezone attached to a lock with Monday - Friday; 10 AM - 5 PM schedule, the system does not again allow users to attach an ARO with overlapping schedule (e.g. Friday - Monday; 8 AM - 11 AM), because the time and day overlap on Monday and Friday between 10AM and 11 AM.
-
- 7 Now select the lockdown you want to attach to this lock. Click the + sign. The Select **Lockdown** window opens.




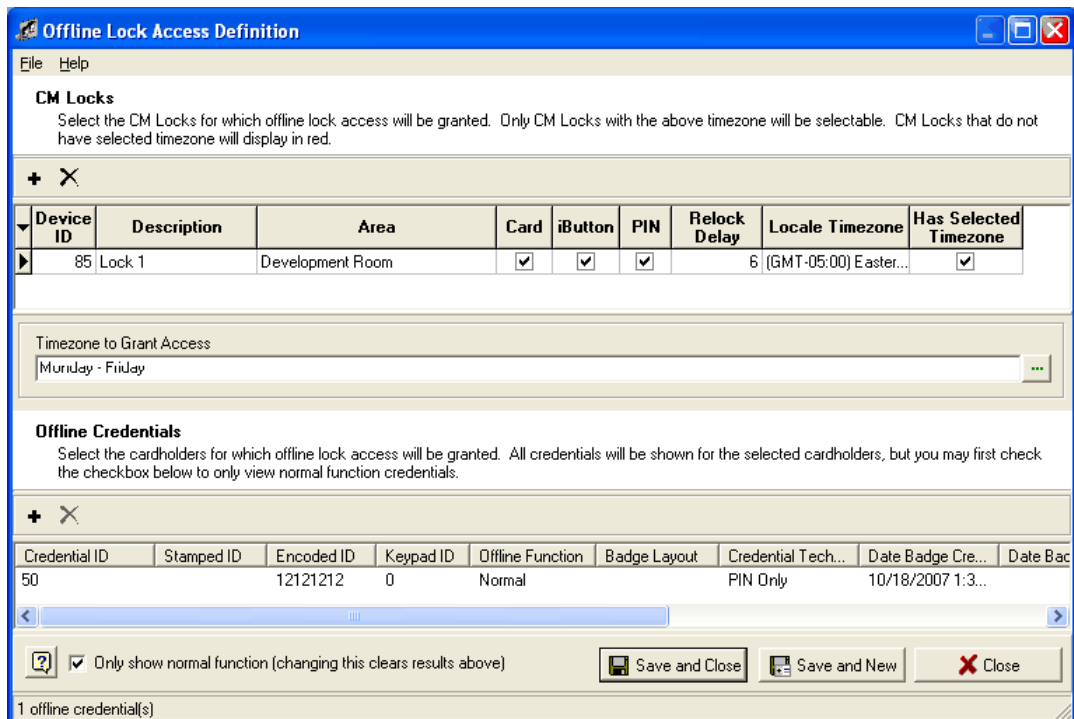
- 8 Click on the expand button near the **Lockdown** field to select a pre-defined lockdown. The **Create Lockdown** button allows you to define a new lockdown. Note that you cannot attach lockdowns with the same time schedule to an offline lock. See the Lockdown Definition section for further details.
- 9 Select **Save and Close** to save the information and close the dialog. Select **Save and New** to save the current information and enter new information. Select **Close** to close the dialog.

Note: No information is saved until the user clicks the **Save and Close**, **Save and New**, or **Save** buttons. If the user exists without saving, they will lose any selected holidays or time zones that were added or removed during that session.

This Grid displays all CM locks defined in the system that the user has at least read only permissions to. These permissions are determined by the area the lock is attached to. If the user has no permissions to the area the lock is attached to, they will not be able to see that lock. This rule is applicable to the option **CM Locks by Area Tree** also.

Adding Credentials to the Lock

If a lock is using only Magstripe and Pin credentials, while adding credentials, only those credential types are available for selection. Click the  button (Create access records for selected records) located on the grid window of System Manager, the **Offline Lock Access Definition** window is displayed. Select the timezone at which access is allowed. Click the + sign in the Offline Credentials section, and only those type of credentials that are specified in the CM Lock Definition window are available for selection.



The screenshot shows the 'Offline Lock Access Definition' window. It has a menu bar with 'File' and 'Help'. Below is a section titled 'CM Locks' with instructions: 'Select the CM Locks for which offline lock access will be granted. Only CM Locks with the above timezone will be selectable. CM Locks that do not have selected timezone will display in red.' There are '+' and '-' buttons. A table lists CM Locks:

Device ID	Description	Area	Card	iButton	PIN	Relock Delay	Locale Timezone	Has Selected Timezone
85	Lock 1	Development Room	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		6 (GMT-05:00) Easter...	<input checked="" type="checkbox"/>

Below the table is a 'Timezone to Grant Access' dropdown menu showing 'Monday - Friday'. Another section titled 'Offline Credentials' has instructions: 'Select the cardholders for which offline lock access will be granted. All credentials will be shown for the selected cardholders, but you may first check the checkbox below to only view normal function credentials.' There are '+' and '-' buttons. A table lists offline credentials:

Credential ID	Stamped ID	Encoded ID	Keypad ID	Offline Function	Badge Layout	Credential Tech...	Date Badge Cre...	Date Bac
50		12121212	0	Normal		PIN Only	10/18/2007 1:3...	

At the bottom, there is a checkbox labeled 'Only show normal function (changing this clears results above)' which is checked. Buttons for 'Save and Close', 'Save and New', and 'Close' are present. A status bar at the bottom indicates '1 offline credential(s)'.

If you select multiple locks that support both Magnetic Stripe and Proximity Credentials for defining offline access, the offline credential tab lists both the type of credentials, but will attach only supported credentials to the corresponding lock. A report will be generated for the failed attempts to add credentials to the lock.

If a lock has mixed card credential types such as a proximity and Magstripe credential attached on one lock, when upgrading the system, neither the proximity nor Magstripe radio button is selected. The user is given the option to determine which type of Card credential the lock should use. The user is informed of the number of Magstripe and Proximity credentials that is in use, and is prompted to select either Magstripe or Proximity credential types in order to save modifications to the lock. When the user clicks the Save button, he/she is prompted to remove invalid credentials from the lock. Based on the credential type selected, the user can remove the conflicting credentials from the lock.

Select the checkbox **Only show normal function** in order for the Search to find only credentials with Normal function.

View Access Records

Follow these instructions to view the access records for a particular CM lock:

- 1 Select an offline lock from the Grid and then right click to bring up a menu. Select **View Access Records** option.



- 2 You can also access this option by clicking the **View selected device access records** button on the navigation bar.
- 3 The system displays access records attached to the selected offline lock.

Note: The user must have read/write permissions to both System Manager and to the System Manager security item *Edit Offline Locks*, in order to insert, update, or delete access records in this dialog.

Editing CM Lock Definition

- 1 To edit a lock definition, select **CM Locks** from the Option bar and double click on the definition you want to edit from the Grid view. You can also select **View>Grid Windows>Devices>CM Locks>View All CM Locks**.
- 2 The **CM Lock Definition** window displays the selected definition. Make the necessary changes and, click **Save and Close**.

Also, a button to Create a new CM Lock duplicating information from the current lock is available at the bottom left corner of the window. Click on this tab to open the **Duplicate CM Lock** window. This feature is discussed in the ***Duplicate CM Lock Definition*** (on page 126) section.

Note: The duplicate option is only enabled during edit mode. When performing a duplicate option, only saved information will be duplicated. If a lock was changed and then not saved and then duplicated, the new lock will receive the duplicated lock's last saved information.

Editing Timezone Intervals for CM Locks

The user can modify the timezone intervals that are attached to a lock. Double click on the record you want to modify and make necessary changes in the **Timezone Interval Definition** window. Save your record.

Timezones with one interval

While the system allows to modify the time, days and holidays attached to a lock, it does not allow the user delete any of this information. If the timezone has only one interval, it cannot be deleted. Intervals can be deleted only if the timezone has two intervals.

Timezones with two intervals

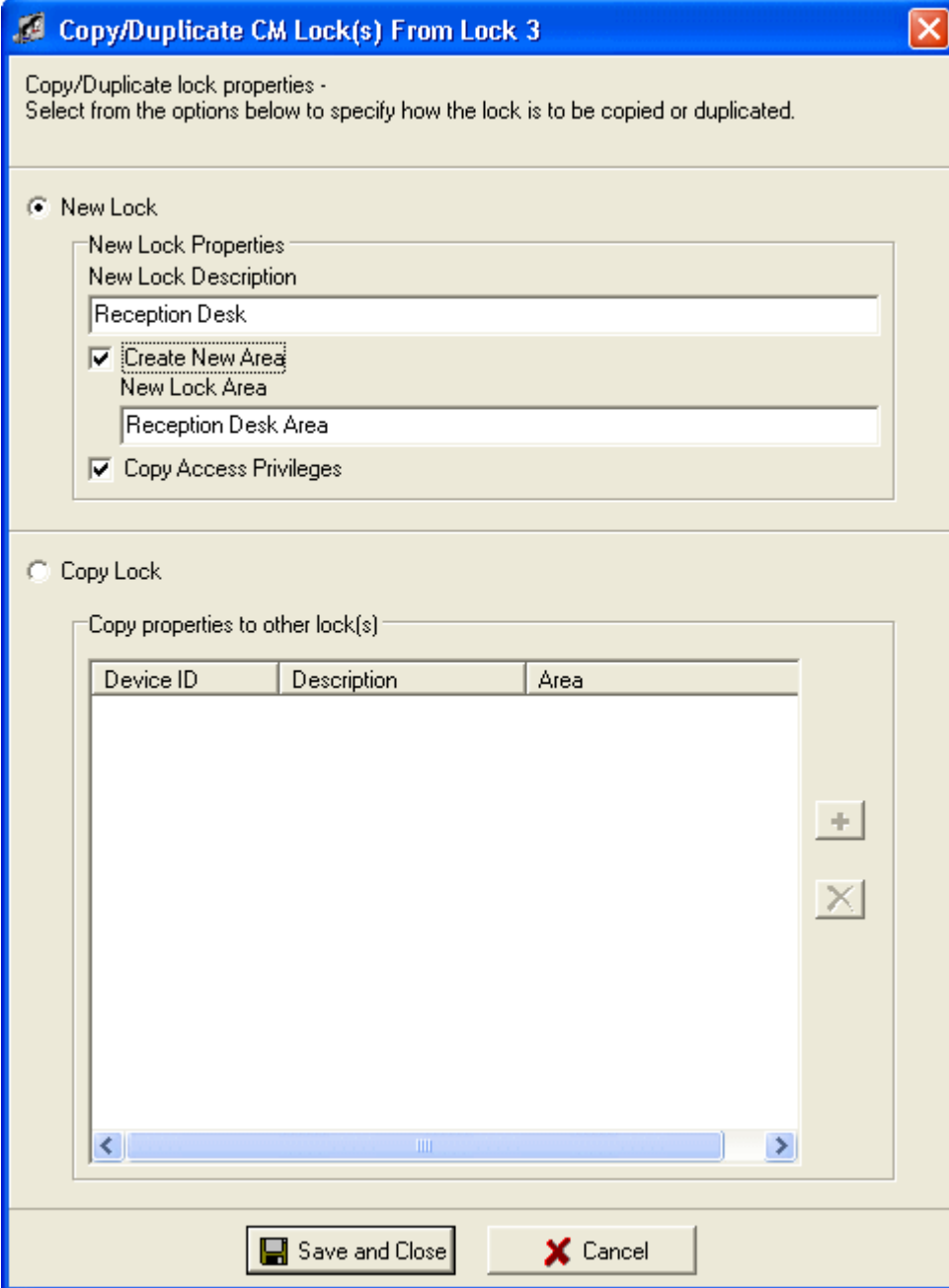
For timezones spanning midnight, the system will not allow the user to modify the interval time that starts at 12.00 am and ends at 11.59.59 pm. The start time of the first interval and the stop time of the second interval can be modified regardless of whether it is attached to a lock or not. In order to modify the weekdays of the timezone that spans midnight, you need to delete one interval, change the weekdays of the existing interval, and then add the second interval.

Duplicate CM Lock Definition

The duplicate feature allows users to duplicate all the properties attached to a lock along with the area access rights.

Note: In order to copy properties of a lock to another lock, both locks must be of the same model and must use the same credential type.

- 1 Select a CM Lock and click on the **Duplicate Selected Record** button located in the toolbar. This opens the **Copy/Duplicate CM Lock** window. This window is also accessible while editing a CM Lock (double click on a lock definition).



The dialog box is titled "Copy/Duplicate CM Lock(s) From Lock 3". It contains a message: "Copy/Duplicate lock properties - Select from the options below to specify how the lock is to be copied or duplicated." There are two radio buttons: "New Lock" (selected) and "Copy Lock".

Under "New Lock", there is a section "New Lock Properties" with the following fields and options:

- "New Lock Description" with a text box containing "Reception Desk".
- A checked checkbox "Create New Area" with a sub-section "New Lock Area" containing a text box with "Reception Desk Area".
- A checked checkbox "Copy Access Privileges".

Under "Copy Lock", there is a section "Copy properties to other lock(s)" containing a table with three columns: "Device ID", "Description", and "Area". The table is currently empty. To the right of the table are two buttons: a "+" button and a "X" button. Below the table is a horizontal scrollbar.

At the bottom of the dialog are two buttons: "Save and Close" and "Cancel".

There are two ways to duplicate the lock. The first option is creating a new lock duplicating the properties of an existing lock by using the **New Lock** button.

- 2 Click on the **New Lock** button, and the New Lock Properties section is enabled. Enter a description for the new lock.

Create New Area - Enable (enabled by default) this option if you want to create a new area for the new lock. Enter the description for the new area in the field. By default the **New Lock Area** field will be filled with the New Lock name + Area.

Example: If the new lock is named Reception Desk then when the cursor is put into the New Lock Area field it will automatically say Reception Desk Area.

Note: If user does not have at least read/write permission, they cannot add a new area.

- 3 **Copy Access Privileges** - This option allows you to copy the access privileges of the existing lock to the new lock. Click **Save and Close**. The **CM Lock Definition** window opens with the new lock information you entered **Copy/Duplicate CM Lock** window.

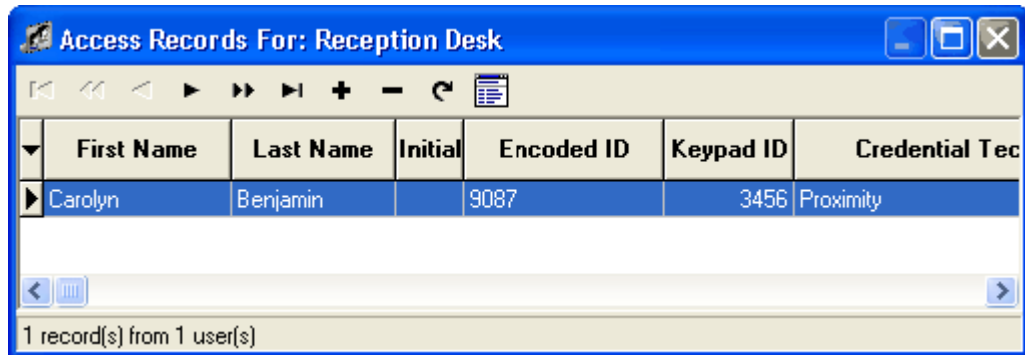
The image shows the 'CM Lock Definition' window with the following fields and options:

- Description:** Reception Desk
- Notes:** (Empty text area)
- Model:** CM Lock -- 1000 Credentials
- Area:** Reception Desk Area
- Locale Timezone:** (GMT-04:00) Atlantic Time (Canada)
- Relock Delay:** 6
- Credential Type:**
 - ☒ Card
 - ☒ iButton
 - ☐ PIN
 - ☐ Magstripe
 - ☐ Proximity
- Magstripe Template:** Default Template
- ☐ Automatic Overrides Credential Enabled

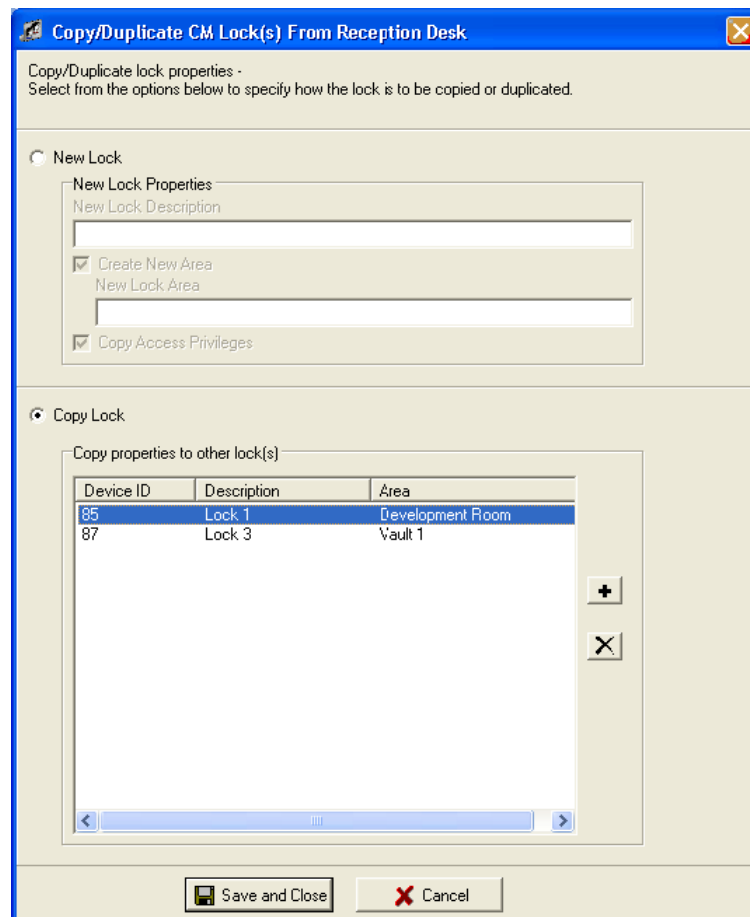
Buttons at the bottom: ? (Help), [icon] (Save and Close), [icon] (Save and New), X (Close).

Explore all the tabs available on this window to verify that all the properties of the existing lock are copied to the new lock. You can update any of this information, and the Save and Close button will be enabled to update your changes in the system.

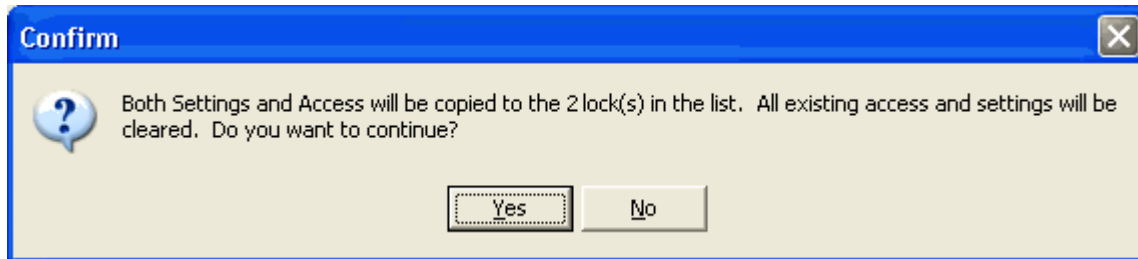
Also click on the **View Access Records** button (System Manager>Hardware Definitions>CM Locks>Grid section) to view the access records that are copied from the existing lock. You can also add/remove more credentials to this lock by using the appropriate toolbar icons (+ or - signs).



- 4 The second option is copying the properties and access privileges of a lock to another existing lock(s). Select a lock that you want to copy, and open the Copy/Duplicate CM Lock window. Click on the Copy Lock button. Now click on the + sign and add the lock(s) you want to update. Clicking the X button removes the selected lock(s) from the list.



- 5 Click **Save and Close**. The following confirmation message is displayed.



- 6 Click **Yes** to copy the settings and access of the selected lock to the target locks. The properties and access privileges attached to the target locks will be overwritten. Once you click Yes, a confirmation message shows the number of locks that are updated.

Define Campus Locks

Refer to the section on Campus Locks for further information on defining Campus Locks.

Magstripe Template Definition

The **Schlage SMS** allows the user to define a Magstripe Template. The Magstripe template field allows the user to enable up to 16 of the 37 digits of the Magstripe template. Enabled digits will display in blue to indicate they are enabled. The 1 or 2 digits representing the issue code display in red. The issue code is 1 or 2 of the enabled digits. If the digits are not enabled, then the issue code offset is not valid.

Follow these steps to define a Magstripe template:

- 1 In the **System Manager** main window, select **Edit>Magstripe Template**.
- 2 The **Magstripe Template** dialog opens. This allows the user to insert, modify, and delete Magstripe templates. Factory set templates display in a light blue color. These templates cannot be deleted and, only the Description and Notes fields can be modified.
- 3 Select the + sign. The **Magstripe Template Definition** dialog allows the user to define a new template.
 - a) Enter a description (this is a mandatory field) and notes for the new template. The description field allows a maximum of 64 characters. The notes field allows a maximum of 255 characters.
 - b) Enable the digits that you want to use for the Magstripe card. Enabled digits will display in blue to indicate they are enabled. If the user attempts to enable more than 16 digits a message is displayed.
 - c) The user can enable or disable the issue code offset by using the **Issue Code Offset Enabled** checkbox. The 1 or 2 digits representing the issue code will display in red. If the digits are not enabled, then the issue code offset is not valid. If the issue code offset is enabled, there is a user friendly control which helps the user select one.

- d) To unselect all the digits of the template, right click and select the menu item **Deselect All**, which disables all the selected digits.

Magstripe Template Definition

File Search Help

Description
IRT Template

Notes

Magstripe Template

1	2	3	4	5	6	7	8	9	10	11	12	13	14
15	16	17	18	19	20	21	22	23	24	25	26	27	28
29	30	31	32	33	34	35	36	37					

☐ Issue Code Offset Enabled

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Issue code offset is disabled

Save and Close Save and New Close

- e) The caption below the issue code offset control displays what the issue code is.

Note: Only the odd positioned digits can be selected as the issue code offset because of limitations of the firmware.

- f) The **Save and Close** saves the current record and then closes the dialog. The **Save and New** button saves the current record and then creates a blank one. The **Close** button closes the dialog without saving the current record. The grid supports all the basic functions (sorting, column resizing and moving, column saving, and exporting the data).

Note: The dialog saves the size and position when closed and re-opened.

Editing a Magstripe Template

- To edit a template, select the record and double click on it. The **Magstripe Template Definition** window displays the current record. Make your modifications and, click **Save and Close**.

Note: When you make changes to a Magstripe template that is already in use, you get a warning message saying how many locks and credentials are affected. If you continue with the change, the Magstripe CM Lock Credentials that were enrolled using the auto retrieve button will have their encoded ID re calculated with the new template. If the credentials were manually entered, no changes are made to the encoded ID and the credentials are invalid.

Deleting a Record

- 1 Select the record you want to delete, and select the minus (delete the current record) sign from the tool bar.
- 2 To delete multiple records at the same time, select the records by holding down the shift key and select the minus sign.

Refresh

The refresh button allows the user to manually refresh the grid if needed. The grid does automatically refresh when the user performs tasks, but the tool bar icon can be used in case another user makes a change.

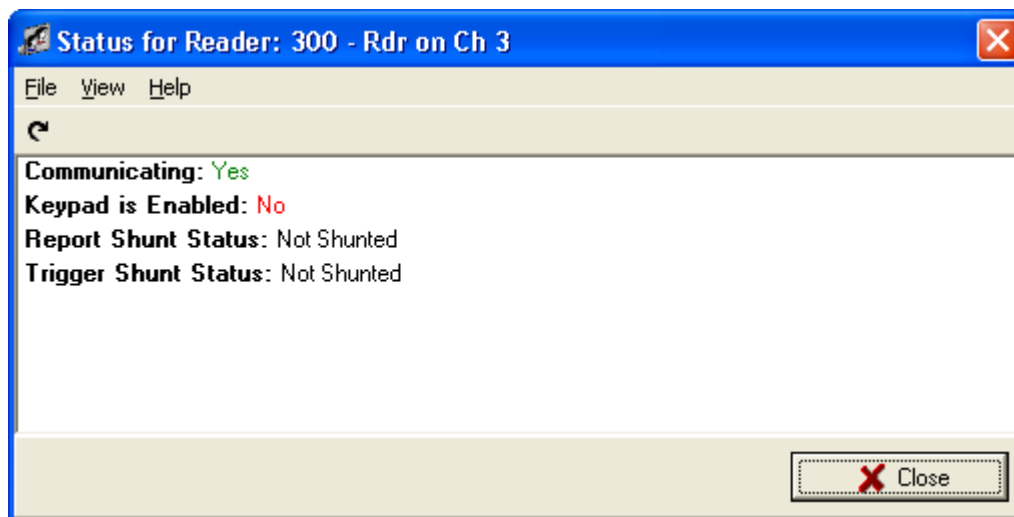
Note: The user must have Read/Write to System Manager in order to add, modify, or delete records.

Device Status

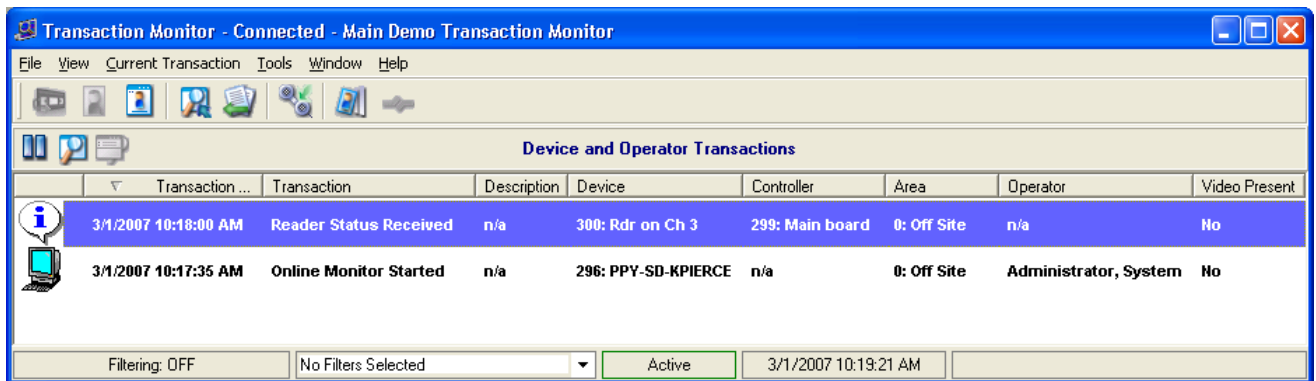
Device status provides the operator a view of a single devices state at any point in time. The user has the option of requesting and receiving status from reader, relay or contact. The status is displayed in a dialog box when it is received.

- 1 Select a device (relay, reader, contact) and click the **View Device** Status icon located at the lower section (grid section) of the main window of System Manager or highlight a device record, right click and select **Device Status** option.
- 2 The **Device Status** dialogue is initiated in order to retrieve the most recent status for that device. Closing and re-opening the dialog requires status to be requested again; therefore, the fields display a message that says, the system is currently retrieving the device status until it has received the status or has timed out until the status is retrieved.

However, opening the dialog initiates the device status request for the selected device automatically.



Status can only be requested from a single device at a time. There will be no grid display of status for multiple devices. Transaction Monitor displays transaction when device status messages are sent to the System Manager application.



Editing records

In System Manager edit menu allows you to edit area states, door types, contact types, reader types, relay types, badge technology, badge status and reader templates.

Note: While editing a record the records that are factory set come up in sky blue color. You cannot insert new records or delete existing records in area states and door types.

- 1 **Area State** - Opens the Area State Definition window that displays all Area States that have been defined. Examples are normal, strike and lock-down. Additions and deletions are not permitted. Modifications can be made in this window.
- 2 **Door Types** - Opens the Door Type Definition window that displays all Door Types. Additions and deletions are not permitted. Examples are pedestrian and car park barrier. Modifications can be made in this window.
- 3 **Contact Type** - Opens the Contact Type Definition window that displays all Contact Types. Examples of contact types are REX and DOD. Additions and deletions are not permitted. Modifications can be made in this window.
- 4 **Reader Types** - Opens the Reader Type Definition window that displays all Reader types that have been defined. Examples are standard reader, entry reader or muster reader. Additions, modifications and deletions can be made in this window.
- 5 **Relay Types** - Opens the Relay Type Definition window that displays all Relays that have been defined. Additions, modifications and deletions can be made in this window.
- 6 **User Types** (see "Defining User Types" on page 466) - Opens the User Type Definition window. The user can enable and label required user types. This option is associated with Campus Locks.
- 7 **Badge Technologies** - Opens the Badge Technologies window that displays all Badge Technologies such as magnetic stripe and proximity. Additions and modifications can be made in this window. Deletions are not permitted.
- 8 **Reader Templates** - Readers are designated as templates when you have additional readers that will use the same or very similar relay, contact, event trigger and override information. A template will duplicate the information so that it does not have to be redefined each time a new reader is added to the database.

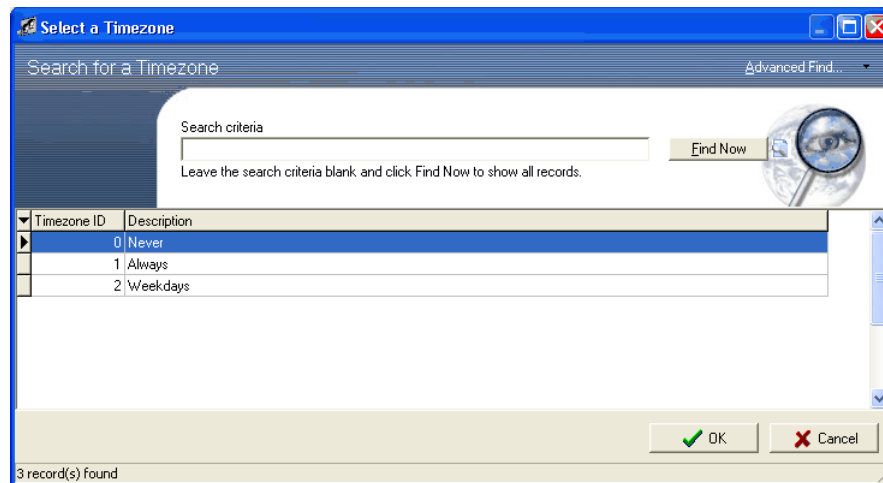
View

The View menu offers two drop down options, Tree Windows and Grid Windows. Each of these options offers additional sub window selections. The Tree Windows are the top tabs of the main screen. The Grid Windows refer to the tabs of the Information Grid that are located on the bottom section of the main screen. The user can open an individual window or can display several pop up screens using this feature.

- 1 **Tree Windows** - The drop down options display pop up screens for the Area Tree, Area Sets, Callback Sets, Cardholder Categories, Hardware Map, Holiday Sets, Site Code Sets and Time zones.
- 2 **Grid Windows** - This option includes sub windows for specific features.
- 3 **Areas** - Offers All Areas and Areas By Area Set.
- 4 **Cardholders** - All Cardholders, Cardholders By Category and Cardholders by Area
- 5 **Devices** - All Readers, All Contacts, All Relays, Readers By Area, Contacts By Area, Relays By Area.
- 6 **Time Zones** - Intervals In Time Zones, Edit Time zone Intervals and Holidays.
- 7 **Callbacks** - Display the Available Callback Number window.
- 8 **Site Codes** - Displays the Available Site Code window.

Search

- 1 Click on **Search** and select **Find** to search for a timezone. The following window opens.



- 2 The **Advanced Find** feature helps the operator to customize the search function. The operator can define the searches and save them for a later use. The saved search criteria is displayed only for the operator who defined it.

Using Advanced Find, you can build the search criteria by selecting appropriate entries from the drop down list box and entering specific value in the value field. You have to select a specific field name, condition and a specific search value.

Advanced Find feature uses Boolean logic to create complex and highly precise searches. Boolean logic uses three connecting operators (NOT, AND OR) to narrow or broaden a search or exclude a term from the search. It is the process of linking criteria to narrow or expand a search through the use of **NOT**, **AND** or **OR**.

The **Advanced Find** feature helps the operator to customize the search function. Operator can define the searches and save them for a later use. The saved search criteria is displayed only for the operator who defined it.

- 3 Click on the **Advanced Find** tab located on the top of the Search window.
- 4 In the **Advanced Find** window define the criteria you want to use.
 - a) If you want to search for Area ID=10, you need first select left parenthesis from the list box.
 - b) Parenthesis can be used to create nested search clauses. Using the Parenthesis one can override the standard order of priority (left to right) for each Boolean statement in the search.
 - c) Select Area ID as the Field Name.
 - d) Select equal to (=) as the condition.
 - e) Enter the value as 10.
 - f) Provide the closing parenthesis at the end.
 - g) If you would like to specify additional search condition you can select AND/OR from the list box.
 - h) If you enable the NOT check box the search result will display all the records except the ones mentioned in the NOT search criterion.

E.g. if you want to search Area IDs between 10 and 20 and between 25 and 30 you can define the search criteria as follows. Use the double parenthesis to nest a search clause.

```
((Area ID>10) AND (Area ID<20))  
OR ((Area ID>25) AND (Area ID<30))
```

When you run the search you will get records corresponding to area ID values 11 to 19 and 26 to 29.

- 5 When you are satisfied with the description, click **Add to List** button. If the criteria is not valid, it is displayed in red under the Where Clause section. When the criteria becomes valid the font color changes to black.
- 6 Highlight the criteria and select **Save** as from the file menu. The **User Searches** window is displayed. The existing Searches are displayed on this window. Now you can either select an existing search and overwrite it or create a new search. To create a new search, click the plus icon. Enter a description for the new search in the **Definition** window. Click **Save and Close**.
- 7 In the **User Searches** window the new search is listed. Click **OK** to return to the Search Criteria tab.
- 8 Click the drop down arrow to the right of the **Advanced Find** button. In the drop down list you can see your saved user searches. Click on the one you defined now. The search results are displayed in the window. You can define as many searches as you want. Each criterion you define should be different from the rest.

Exporting Cardholder Search Results

Cardholder search results can be exported to your hard drive from the **All Cardholders** tab in the following formats: .xml, html, txt, csv (comma separated value).

To export search results to your hard drive,

- 1 Run a search and right click on the search results.
- 2 Click the **Export Results** option from the menu.
- 3 Choose the directory to which you want to save the results. Give a file name. Click the drop down menu to choose an available file format.

- 4 Click **Save** to complete the action and the search results will be saved in your system.

Cardholder Definition

CHAPTER 5

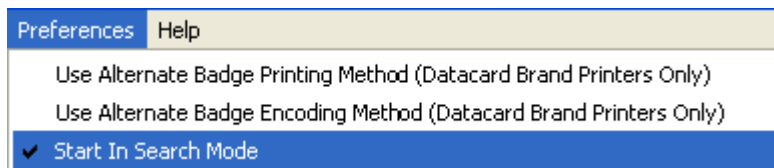
Introduction

The user friendly interface of the Cardholder Definition program allows the user to store the cardholder information easily. The **New Cardholder Wizard** prompts the user for all necessary cardholder data and provides step by step instruction for adding a new cardholder record. The system allows a cardholder to have both online and offline credentials. Offline credentials are used to give access to CM and CL locks. With the help of wizards, all data regarding active and retired credentials, lock access, area access (available only in Schlage Professional and Elite systems), cardholder Categories and e-mail addresses are entered and retrieved effortlessly. The user can capture, edit and store cardholder portraits and signatures. The Portrait Enhancement Utility takes the cropped image, enhances it and then displays a selection of 15 photographs. Images can be exported out of the module and sent to any file on your network. There are also options to duplicate cardholder information and print reports. The Advanced Find method helps the user to achieve accurate search results using either simple or complex search options.

Accessing the application

- 1 Open the **System Launcher** by double clicking the Launcher icon on your desktop or go to **Start>Programs>Schlage SMS> Schlage SMS**.
- 2 The login window opens. Enter your user id and password.
- 3 In the **System Launcher** window, double click on the **Cardholder Definition** icon.

The user can set the Cardholder Definition program to open either in the **Search** mode or in the main screen. This option is set under the **Preferences** menu of the main screen.



To go to the main screen, close the search window, and the program opens the main Cardholder Definition screen. Unselect the **Start In Search Mode** option in order for the program to open the main screen by default.

Working with Cardholder Definition

Credential ID	Stamped ID	Encoded ID	Issue Code	Keypad ID	Badge Layout
3	4564565	8990	1	1234	

The main screen displays the cardholder factory set and user defined fields. The position of the fields are arranged, modified and saved using the UDF Editor module. The lower section of the program displays individual cardholder information regarding badge status, lock access, area access, cardholder category and e-mail addresses. Green, yellow and red color indicators are incorporated into the area access time zone and expiration fields. A green indicator shows valid access, a yellow indicator means the access will expire shortly; and red indicates that access has expired.

The system offers multiple options to add new cardholders into the system. You can use the cardholder wizard, tool bars or main screen to accomplish the same task.

The **Cardholder Wizard** (available only in Schlage Professional and Elite systems) is a step by step feature that prompts you for all necessary cardholder data including badge, area sets, area access, category information, image and signature capture. A second option for inputting cardholders is the **New Cardholder** option. This allows you to input the information directly on the main screen. The **Duplicate Cardholder** option is a quick and simple way to enter multiple cardholders who have the same area access and belong to the cardholder category. The program copies these fields from the previous record to a new cardholder record.

It will also replicate user- defined fields that are marked for duplication in the UDF Editor module. The user can then enter the new cardholder's name, badge and image information.

Removing multiple cardholder records simultaneously is easily accomplished through the **Delete Cardholders** feature. All these features are described in detail later in this document.

Note: We recommend you to explore the tool bars icons, menu bar drop down options, hot keys and tabs to be familiar with all the available options within the program.

Add a new Cardholder

There are two ways to enter new cardholder information. They are, using the **Cardholder Wizard** and the **Add New Cardholder Options**. The Cardholder Wizard will lead you step by step through its screens for cardholder information. The Add Cardholder option allows you to enter information directly on the main screen. However additional steps for image and signature capture are necessary.

New cardholder wizard

Note: Adding cardholders using the wizard is available only in Schlage Professional and Elite systems.

The **Cardholder Wizard** screens prompts you to add cardholder information, user defined fields, to define badges, add area sets and additional areas for access privileges, cardholder categories and image and signature capture.

- 1 Select **File>Cardholder Wizard** option or click the wand icon on the tool bar.
 - a) The **New Cardholder** wizard shows all the available fields (the fields that you see on the main screen) including the user defined fields.
 - b) Last Name is a required field on the first screen. If a User Defined field has been defined in the **UDF Editor** as “Required”, then UDF fields must also be entered as well.

User Defined Fields are additional cardholder fields; examples of UDFs are Nick Name, Social Security Number or Phone Extension. Please refer to the **UDF Editor** section for more information. You may type in any of these fields to modify the information. In addition, the date fields offer a drop down calendar. Use the down arrow to scroll for additional fields on the page.
 - c) The portrait capture date and signature capture dates are disabled as these dates are entered automatically while adding portrait and signature.

- d) If you want to block the cardholder's Area Access privileges check the box near the option **Access Blocked**.
 - e) To enable anti-pass back feature check the box near the **Controlled Anti-pass back** option. If this field is unchecked the card is considered as a master card and it will override the anti-pass back, global anti-pass back rules of the card readers. The card can be used anywhere, any number of times.
- 2 **Anti-Pass Back** - Anti-pass back is a function that prevents cardholders from passing their card to another person for illegal entry. The same card cannot be used at an entry or exit reader twice in a row. In other words, once a card is presented at an entry reader, it must then be presented at an exit reader. If a card is presented twice in a row at the same type of reader, no access will be granted. The Transaction Monitor will display an anti-pass back violation transaction. It is commonly used at car park barriers and turnstiles.
 - 3 If the cardholder is a disabled person, select the option **Special Access Privileges**. The system identifies valid card reads from cardholder's with special access privileges in order to allow access through specific doors with longer GO Relay times (time door strike shall remain energized). The Transaction Monitor displays transactions that differentiate a normal card swipe with a card swipe from a person with special access privileges. If the field **Special Access Privileges** is selected, when the cardholder swipes his/her card the following transactions are displayed instead of the normal “Valid Access” type transactions.

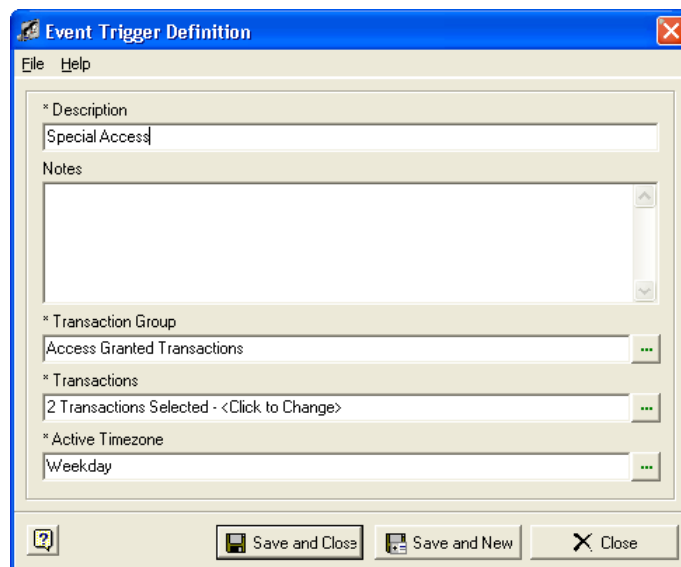
- Valid Access – Special access privileges.
- Valid Entry – Special access privileges
- Valid Exit – Special access privileges

Setting up Special Access Privileges

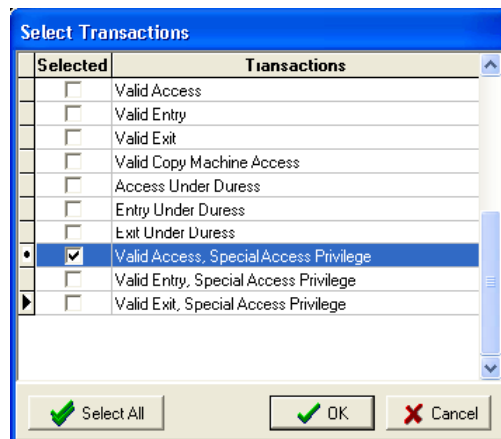
- Select the Special Access Privileges check box in the **Cardholder Definition** window.
- In System Manager, select the reader you want to set up for assigning special access privileges. You need to define the Event Triggers and Actions with increased access time for allowing the disabled person to access through the door without any inconvenience.
- With the reader selected, click on the **Event Trigger Definition** button from the toolbar.



- The **Event Triggers for** window opens. Click on the + sign on the **Event Triggers** section to define a new event trigger for Special Access Privileges feature.



- e) Enter a description. Select the **Access Granted Transactions** group by clicking on the browse button. In the Access Granted Transactions list, there are three transactions available for special access. If the reader you are defining event triggers for is an entry or exit reader, you must select either **Valid Entry** or **Valid Exit** transactions. These types of readers are used for creating evacuation reports. Click **OK**.

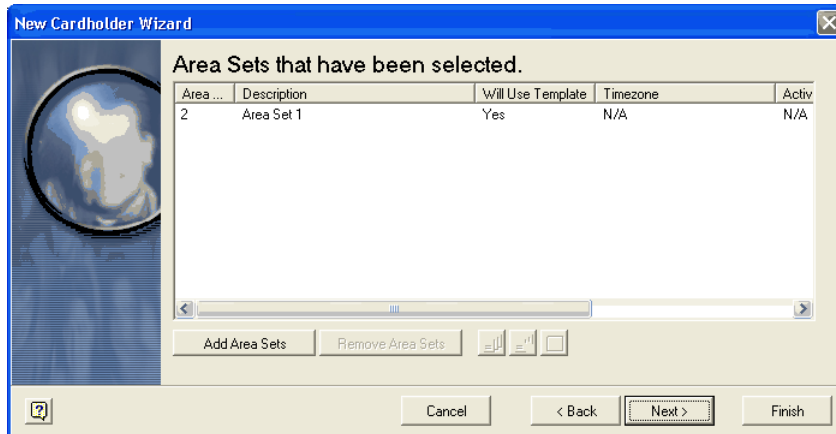


- f) Click **Save and Close** on the Event Trigger Definition window.
- g) Now define the action items for the event trigger. First action you need to define is **Energize Relay**. Select the device and command to execute. The duration must be set to longer time period than the usual settings to give enough time for the disabled person to go through the door without generating any alarms (E.G 20 seconds). The second command is Turn **LED Green**. Here also set the duration to a longer time. The duration setting sets the amount of seconds the relay will be energized. There are two Commands that have to be programmed for the DOD Contact. The first is **Contact Reporting Disabled**. This prevents the **Contact Active** transaction, which may be an Alarm, from being sent for the amount of time that is set in the **Duration of Seconds** field. Again set the Duration time for 20 seconds. Once you have defined all the actions for the trigger, click the **Close** button to exit the window.
- 4 You can continue add new cardholder process in the Cardholder Definitions program.

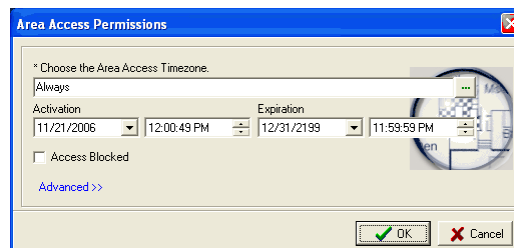
Assigning Areas and Area Sets

Note: Area access functionality is available only in Schlage Professional and Enterprise systems.

- 1 Next, select the **Area Sets** that you want to assign to the cardholder.



- a) Click **Add Area Sets**.
- b) Choose the Area Sets from the **Select Area Sets** window. You can use the Search feature to locate Area Sets easily. Click **OK**.
- c) Click **Next** on the New Cardholder Wizard.
- d) If you want to assign any other Areas additionally click **Add Areas**. Select the Areas and click **OK**.
- e) Now select the Time zone, activation and expiration dates for the Areas. You can open the calendar using the drop down arrow to select the dates. Use the up and down arrow to adjust the time.



- f) Click **Next** on the New Cardholder Wizard.
- 2 **File>Area Access> Add Area Access** option activates the Area Access wizard. There are four different options available on this window.
 - a) **Remove Area Sets** - Removes the Area Set from the cardholder's record.
 - b) **Set the selected records so that they use the stored template values** - This uses the template values for Area Access permissions that have been defined in the System Manager module.
 - c) **Set the selected records so that they do not use the stored template values** - Allows the user to change time zone, expiration values, area state and door types associated with the Area Access permissions for the specific cardholder.
 - d) **Edit access permissions on the selected Area set** - Allows user to change the Area Set's access permission for the specific cardholder, provided you have chosen not to use the stored template values.

- e) Your selections will be highlighted in blue color. After clicking **OK**, the wizard will return to the Area Set window.
- 3 To delete **Area Access**, select an Area from the **Area Access** tab and choose delete.
-
- Note:** The **Area Access** tab in the cardholder main window displays only Areas; it will not display the Area Sets assigned to that cardholder. This means that individual Areas that are members of an Area Set are listed in the cardholder's Area Access tab. An Area will only display one time in the Area Access tab regardless of the fact that it may be in multiple Area Sets that have been assigned to a card. The three buttons are Add Areas, Remove Areas and Edit Areas. Use the **Add Area** window when a cardholder needs access to a specific area and that Area is not associated with any Area Sets that you have assigned to the cardholder. You may want to skip this screen until you can review the Area Access tab.
-
- 4 Select **Next** to skip this step.
- 5 In the **Area Search** screen, type the area name in the criteria field or use **Find Now** to display all areas that have been defined.
- 6 Highlight the Area and click **OK**. To add multiple Areas, hold the control key down while you make your selections.
- 7 Click **OK** to display the Areas that have been selected.

Modify Area Access

- 1 Now, add this cardholder to any cardholder category that is already defined in the system. You can assign a cardholder to any number of cardholder categories.
- a) Click **Add Categories**. Select a category from the list and click **OK**. Add any number of categories you want. Click **Remove Categories** to delete any selected categories.
- b) Select **File>Categories>Add to Category** allows the user to add a cardholder record to a cardholder category list.
- c) Select **File>Categories>Select a Category** to delete a cardholder from a category.

Area Access

- 1 The **Area Access Permission** window prompts you for **Timezone and Access Expiration**. To select a different Time zone, use the browse button. To change the date, use the drop down arrow to access the calendar. The up and down arrows will modify the time field.
- 2 Click the **Advanced** button to display all Area States and Door Types.
-
- Note:** If the Area Set(s) you selected is using an Area Access template, the template values will be automatically assigned to the cardholder. The template is defined and assigned during the Area Set definition section in the System Manager.
-
- 3 To assign a time zone and the access expiration time, on the **Area Access Permissions** window, choose the Area Access Time zone. Select access expiration date and time. Click the down arrow near the date field to display the calendar. Adjust the time using the up and down arrows.
- 4 If you want to block the access, select the check box near the **Access Blocked** field.
- 5 Click **OK**.

Portrait Capture

Next step is capturing the portrait of the cardholder. Select **Capture** to display the **Cardholder Image** window. Under the **Source** field, your choices are **From File**, **From TWAIN Device** or **From FlashbusMV**. Select **Capture** on the Cardholder Image screen; the photograph is displayed. Tool bar icons offer **Crop Image** or **Show Crop Rubber band** options. The rubber band is used to display a red dotted line. Drag the rubber band to the crop position of your choice then select the Crop Image icon. **Save**, **Cancel**, **Edit** and **Refresh** are not available at this point because the image is stored in memory. Look under the Tools menu for image and cropping choices.

- a) **Capture Image** - Click this button to capture the image using the default chosen in the System Manager Settings module. The choices are File, Twain Device or Flash Bus.
- b) **Crop Image** - Opens the Portrait Enhancement Utility. Before selecting this option, verify that your Crop Rubber band is placed on the image where you want to crop the photograph.
- c) **Cropping Rectangle** - Displays the Crop Rubber band on the image. Drag and resize the rectangle into the position that you want the image to be cropped.
- d) **Portrait Image Enhancer** - This feature is enabled in the System Manager Settings module under the Schlage Image Settings tab. When a portrait is cropped, the user is presented with a selection of 15 pictures. Using the Decrease and Increase buttons on the bottom, left of the screen will modify the pictures to make them lighter or darker. Click on the picture of your choice. The window closes and you are returned to the New Cardholder wizard Cardholder Image screen. If you are satisfied with the image select the **Save** icon.
- e) Save your changes and close the **Cardholder Image** window. The cardholder portrait is displayed on the New Cardholder Wizard.

Signature Capture

Next, you can capture the signature of the cardholder. Click **Capture**. The **Source** choices are File, TWAIN Device or Schlage. If you select the option Schlage, you need to have a signature pad connected to the COM Port of your PC. If you select the option From File, the Signature folder is displayed by default. Select the file and click **Open**. The signature is displayed on the Cardholder signature screen. Refer to the previous section in this manual for the tool bar options. Save your changes and close the window. click **Next** on the New Cardholder Wizard.

Credential Definition

Adding credentials is the final step in the cardholder insert wizard. Cardholders may be assigned more than one active credential including one blank badge (a credential without an encoded ID or a stamped ID). **Schlage SMS** supports both active online credentials and offline credentials (offline credentials are used for the offline locks). The offline device does not communicate directly with the host controller. The manual programming of the device shall occur at the reader location.

The system allows you to define same online and offline credentials for cardholders.

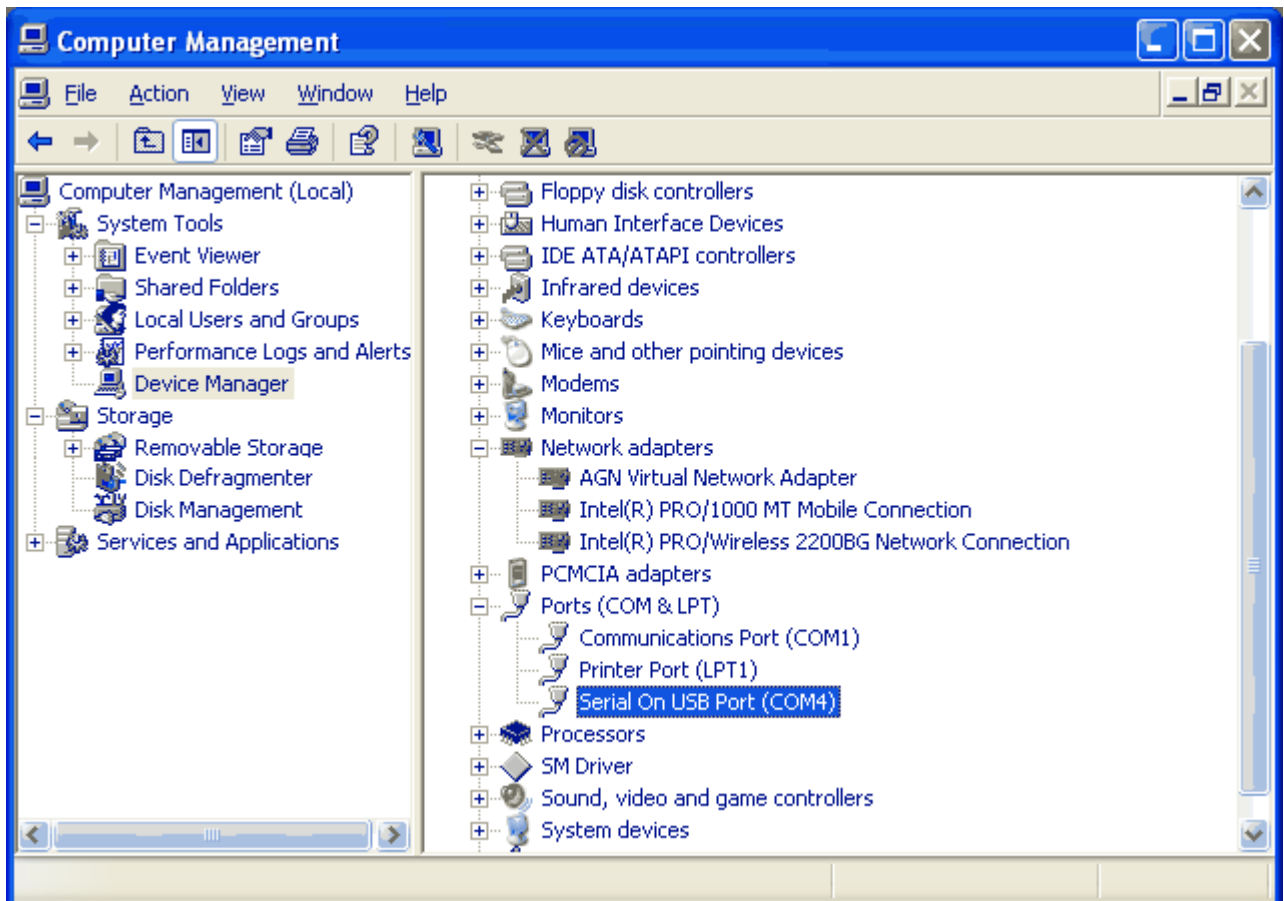
Note: **Schlage Enrollment Reader** allows you to enroll both online and offline credentials. This device has Magstripe, proximity, and iButton read heads and can be connected to a PC running the **Schlage SMS** software via a serial port or via a serial->USB adapter that is included with the hardware.

Setting up Schlage Enrollment Reader

The credential data is retrieved using either Schlage Enrollment Reader or Offline Enrollment Reader. This enrollment reader is connected to a PC running the Schlage SMS software via a serial port or via an included serial->USB adapter. To use the USB Port Adapter, you must first install the driver software on your computer. Once the driver has successfully installed, you will need to restart your computer. This device has Magstripe, Proximity, and iButton read heads.

Connecting the hardware and determining the COM Port

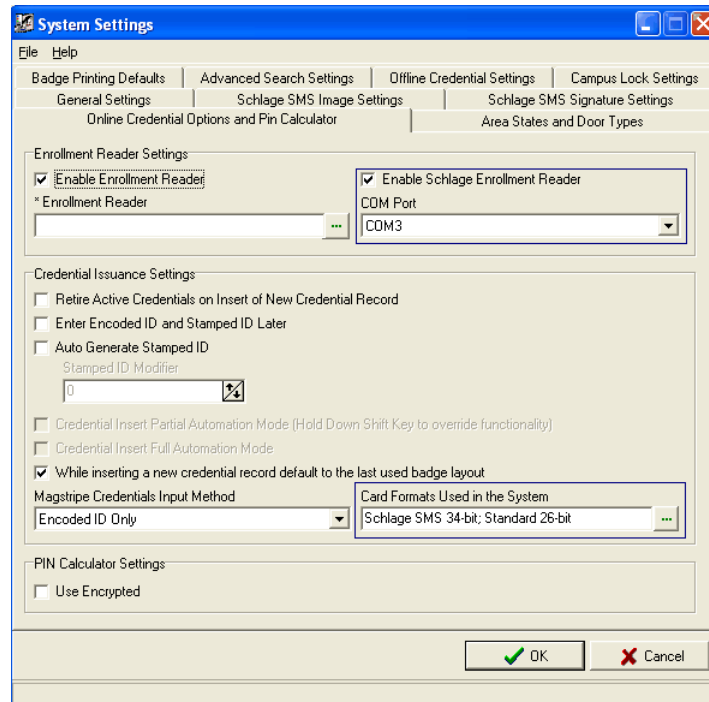
- 1 Connect the USB Adapter to the USB Port of your computer.
- 2 Go to My Computer. Right click on **My Computer**, select **Manage**. This opens the **Computer Management** screen.
- 3 On the Computer Management screen, select **Device Manager>Ports (COM and LPT)>Serial on USB Port (COM #)**. It shows the specific COM Port that is used to connect the Enrollment reader.



Setting up the Enrollment Reader in Schlage SMS

- 1 Open System Settings program. Choose the tab, **Online Credential Options and Pin Calculator**.

- 2 Under the **Enrollment Reader Settings**, select **Enable Schlage Enrollment Reader**.
- 3 Now select the **COM Port** that is used to connect the Enrollment Reader. This Com Port must be the same that you have determined in the previous step.
- 4 In order to add credentials, the system needs to know the format of the credential. Click the browse button near the **Card Formats Used in the System** field. It opens the Card Formats Used in the System window. Choose the card formats that you will be using.



Active Online Credentials

Note: Online credential functionality is available only in Schlage Premier and Enterprise systems.

Active online credentials are used for the readers that communicate directly with the host controller. Follow these steps to define the online credentials.

Add credentials

- 1 Select the tab **Active Online Credentials**. Select **Add Credential** to open the **Credential Definition** screen.

Note: One credential per cardholder can be added without entering a stamped ID or an encoded ID. Check the option “Enter the Stamped ID and the Encoded ID Later”. If the current cardholder already has a blank badge (a badge without a stamped ID or encoded ID) the Credential Definition window will not allow the user to create another blank badge.

- a) **Credential Technology** - Click on the expand button to select the badge technology used for this credential. Magnetic Stripe, Barium Ferrite, Proximity, iButton and PIN Only are available options.
- b) **Stamped ID** is the pre-printed number located on the back of the cardholder's badge.
- c) **Encoded ID** - Encoded ID is a unique numeric value that is required to add a credential to a cardholder record. For instance, a proximity card has a chip programmed with the number. A magnetic stripe card will have the number embedded in the stripe. The maximum value you can enter is 4294967295 for online credentials.
- d) **Issue Code** counts the number of badges issued to an individual cardholder. The original credential will have Issue Code zero (0).
- e) **Badge Layout** -This is a required field. Badge Layout displays the list of layouts that have been created in the Badge Creation module.

Note: Privileges to select, view or print badges will be based on the operator's security group permissions set in the System Security Module. When permission to a badge layout equals none, selecting, viewing or printing that layout will be unavailable.

- f) Once you fill in the required fields, select **Save and Close**. Click **Save and New** to add another badge. The information will display in the grid window. Once you are done with adding badges click **Finish**.

Active Credential Options

There are eight options available under the Active Credentials sub-menu. Selecting from the Active Badge sub-menu links to badge fields and opens the **Active Credential** tab.

- 1 Select **File>Active Credentials**. The following are the menu options.
 - a) **Add Credential** - Opens the **Credential Definition** window.
 - b) **Retire Credential** - Highlight a badge then select this option to remove it from the Active Online Credential tab and write it to the **Retired Credential** tab.
 - c) **Reset Anti pass back State** - Returns the cardholder's anti pass back state to neutral.
 - d) **Select Credential Layout** - Opens the **Credential Layout Description** window that allows the user to select a different layout.

- e) **Print Credential** - Allows user to send the highlighted credential to either the default credential printer or a print queue.
- f) **Calculate Keypad Pin** - Uses the Encoded ID of the highlighted badge to calculate a PIN number. Standard or Schlage PIN Encryption is defined in the **System Settings** module.
- g) **Edit Badge** - Click on this option to edit badge technology and badge layout. Stamped ID, Encoded ID and Issue Codes are displayed as Read Only fields.

Offline Credentials

The **Schlage SMS** supports offline readers (CM Locks and Campus Locks) which do not communicate with the host controller directly. So it is necessary to do manual programming at the reader location. The user can create necessary downloadable files and upload to a pocket PC. The data is transferred to a PDA by connecting to the serial communication port of the PC. The programming of doors is accomplished by connecting a **CIP** (Computer Interface PAK cable) from the laptop/PDA to the iButton ports of the lock. The system will not allow the users to assign different card technologies (Magstripe, Proximity) on the same lock. For example, if a Magstripe credential is already assigned to a lock, the system will not allow the user to assign a proximity card to the same lock and vice versa.

CM lock credential definition

Follow these steps to define CM Lock Credentials for cardholders. The first step in defining CM lock credentials is setting up the Proximity and Magstripe card formats used in the system. This is set up in the **System Settings** program. Custom card formats can be defined using the **Card Format Editor** application. If the card format is unknown, the user can enter that card either by raw data or via an enrollment reader (Schlage Enrollment Reader or Offline Enrollment Reader). The system saves the credential without deriving the Encoded ID, and this credential can be used only on offline locks. It will not function on online locks.

The card formats can be selected using **System Settings>Offline Credential Settings>Card Formats Used in the System** option.

Please refer to **Card Format Editor** section for further information on defining custom card formats.

There are four (4) credential technologies available for creating CM Lock Credentials. They are:

- Magnetic Stripe
- Proximity
- PIN Only
- iButton

Magnetic stripe and Proximity credential definition

Once you have set up the card formats in the system, you can start adding the credentials. If you have defined a card format without a site code, you cannot manually enter the Encoded ID.

- 1 Select the **Offline Credential** tab. To define a new offline credential, select **Add CM Lock Credential**.

Note: This field will be visible only if the user has at least read only rights to the System Manager security item "Badges" and has at least read only permissions to one of the cardholder fields in the grid. If these conditions are not met, this field and the corresponding main menu options (File>Offline Credentials) will not be available. Due to this the File>Offline Credential option is unavailable, even to users with the correct rights, until the user selects the Offline Credential tab.

- 2 The **CM Lock Credential Definition** window opens.

Fill in the following fields:

- a) **Credential Technology** - Select the type of credential technology. You can auto-retrieve the credential technology using a Schlage Enrollment Reader or an Offline Enrollment Reader.

Note: Credential Technology field cannot be changed when you are editing a Credential Definition. The credential must be retired and a new one should be created to change this field. This field must be entered before saving the record.

- **Encoded ID, Raw Data, PIN, or iButton** - This field changes depending on the credential technology you have selected in the previous step. If the Credential Technology you have selected is Magnetic Stripe, Proximity or iButton, this field will be Encoded ID and Raw Data. You can specify the input method in the **System Settings>Offline Credential Settings>Magstripe CM Credential Input method**. Regardless of the input method selected here, both Encoded ID and Raw Data fields are visible on this window. If you select the Input method as **Encoded ID only**, you cannot enter the raw data manually, but you can retrieve the data using an enrollment reader.

- 3 If the input method is not selected in System Settings, both Encoded ID and Raw Data fields are available for selection.

- **Encoded ID-** For this method, you enter a small number, ten digits or less, that is written on the card, usually on the back side of the card. When the Encoded ID method is used, the raw data is automatically generated using the Encoded ID and the Site Code defined for that format. The “Schlage Encoded Card” has the Encoded ID printed on the back. So this method can be used for those cards.

Encoded ID can be entered manually or via a **Schlage Enrollment Reader** or an **Offline Enrollment Reader**. If the system cannot recognize the card format of a card, the Encoded ID must be automatically retrieved (or the user must manually enter the raw data on the card). The system cannot construct the raw data without knowing the Encoded ID (**Setting up Schlage Enrollment Reader** (on page 145)).

If the raw data does not match the selected card formats, the system still saves the data, but Encoded ID will not be derived. The cards without Encoded ID cannot be used on online locks, but these cards will still function on offline locks.

- 4 If you have defined a card format without a site code, you cannot manually enter the Encoded ID. In this case, you must enter the raw data or use the auto retrieve method. The reason is that when the system tries to construct the raw data from the Encoded ID and site code and if there is no site code, the raw data will be incomplete. If the site code is incorrect, the raw data will also be incorrect and the credential will not get access to any locks. If you want to create a credential for a card that has a different site code than the one defined in System Settings for that format, you must enter the raw data or use the auto retrieve method. That is because the system uses the site code extracted from the raw data instead of the one defined in System Settings for those methods.

Note: The site code defined in System Settings is only used when using the encoded ID input method.

- **Raw Data** - Raw data can be entered manually or via an enrollment reader. You must enter all the data from the Magstripe track. The same rules for securing Encoded ID is applied for Raw Data field. If you have Read/Write permissions to Encoded ID field, you can edit Raw Data too.

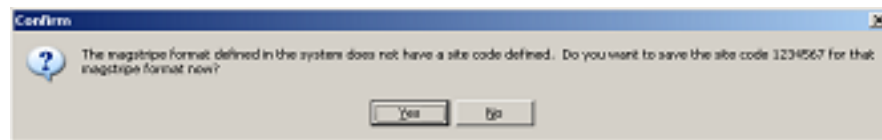
The following are the rules for entering raw data for different credentials:

- a) **Magstripe** - Characters between 0-9 and a few symbols (<, >, =) are valid. The value should be minimum one (1) character long and can contain a maximum of forty (40) characters. The "Locknetic 16 digits mag card w/7-d site code" has the raw data written on the front side of it.

While using the raw data method, you must enter the exact number of characters on the card. If you have the "Locknetic 16 digits mag card w/7-d site code" defined in the System Settings, you must enter sixteen (16) digits or you will get an error message.

"The Magsritpe Credential does not match any of the Magstripe card formats defined in the System".

When you create a Magstripe credential (by using raw data or auto retrieve method) for the first time without a site code, you will be prompted to save the site code for that format. If you click No, then this message will be displayed the next time you create a Magstripe credential and you will still not be able to use the Encoded ID input method.



- b) **Proximity** - For a proximity card, characters between 0-7 are valid and the value must be sixteen (16) characters long.
- c) **iButton** - For iButton credentials, you can use characters between 0-9 and a-f. The value must be sixteen (16) characters long.
- 5 **Auto Retrieve** - This button is used when you are using the offline enrollment reader to extract the data from a card. Click the **Auto Retrieve** button to automatically retrieve the Encoded ID, PIN or iButton ID by attaching an enrollment reader to the computer through a serial port. When the user touches the button or swipes a card at the reader, the system generates the value automatically. The card format and credential technology also can be retrieved using this method. When the manual entry method is used, the user enters the raw data on the card and the system converts it to Encoded ID. When the auto retrieve method is used the complete data on the card is stored in the system.

Note: The Auto-Retrieve button is not applicable to Schlage Enrollment Readers. If you are using Schlage Enrollment Reader, the data will be retrieved when you just swipe the credential or show the credential at the reader. In order for the Schlage Enrollment Reader to function properly, you need to set the COM Port and Card Format correctly in System Settings (**Setting up Schlage Enrollment Reader** (on page 145)).

- 6 Once a credential has been created, you can see Encoded ID and Raw Data on the Cardholder Definitions main screen.
- **Creating iButton CM Credentials**

- 7 **iButton** - The raw data that you enter in this field must be sixteen (16) digits in length and can only have hexadecimal characters (0-9, a-f). You can enter the raw data or automatically retrieve it using Schlage Enrollment Reader or Offline Enrollment Reader. For iButton credentials, Encoded ID cannot be entered manually. The system will not be able to derive the raw data without having information like site code and family code.

- **Creating PIN Only CM Credentials**

- 8 **PIN** - This field is for PIN Only credential types. It must be numeric value between X and 8 digits. X = a setting in System Settings under Offline Credential Settings called Minimum PIN Length. The minimum number of digits that the system allows is three (3). The smaller the minimum length, the smaller the amount of PIN number the system can have.

The system supports both 12 button and 6 button keypads. Also, it is highly recommended to use the **Auto Retrieve** option to generate the PIN, and not to use birth dates or other restricted or easy to guess sources. The system uses the Minimum PIN Length specified in the System Settings while generating the PINs.

- **COM Settings**

- 1 The COM Port must be configured in **System Settings** under the Offline Credential Settings tab called Offline Enrollment Reader COM Port. If the COM Port is not configured correctly, the feature will time out after a set amount of seconds.
- 2 The time-out period can be set under **System Settings> Offline Credential Settings >Offline Enrollment Reader Time-out**. The default is 5 seconds, but you can change this value to have enough time to swipe the credential. The time-out starts as soon as the button is clicked.
- 3 If this feature is used only for proximity cards, the setting in **System Settings>Offline Credential Settings>Proximity Card Format** must be selected. If this field is set incorrectly, an error will occur and the system cannot retrieve the Encoded ID from the badge.

Note: This is a required field.

- a) **Stamped ID** - This field is enabled only for card credential types; it is the number actually printed on the badge.

Generating Stamped ID Or Encoded ID Automatically

The encoded ID and Stamped ID fields can be generated automatically by enabling a setting in System Settings > Offline Credential Settings>Stamped ID Modifier. Enter a value in this field which functions as the modifier of the stamped ID or encoded ID. It works by taking the Encoded ID and subtracting the Stamped ID Modifier to get the Stamped ID and vice versa.

If the above option is enabled, when the Encoded ID is entered by the user, the Stamped ID will automatically be generated using the above calculation. If the Stamped ID is entered by the user, the Encoded ID will be automatically generated.

Note: This field must be between 0 and 2,147,483,647. If the Stamped ID modifier makes this field greater than 2,147,483,647, the field will just be 0 then.

- b) **Keypad ID** -This field is only enabled for Card and iButton types. The **Generate Keypad ID** button can be used to automatically generate the Keypad ID.

Note: Keypad ID also can be generated. It follows the same input rules as the PIN Encoded ID above. Keypad ID value zero means there is no keypad ID. A cardholder can have two credentials with same Encoded IDs as long as the Keypad IDs are different.

- c) **Offline Function** - Click on the expand button to select a function the offline credential will perform when the cardholder presents the credential at the door.

Note: This is a required field.

These are the offline functions available.

Normal - Normal opens a door for a specified time. The time span is defined by the Relock Delay set in the Offline Lock Definition.

Toggle - Toggle opens a door and leaves it open until it is closed again by a toggle credential. It toggles a door between locked and unlocked.

Freeze - Freeze disables the keypad/credential reader. Only credentials set to "Pass Through" can open the door. Use a credential with "Freeze" function to return the door to an operational state. "Freeze" does not lock a door, for example when the door was toggled open.

One Time Use - One Time Use opens the door only once with the Normal function. After the door relocked the credential does not work anymore on this door. It can still work on other doors, until after it was used on these doors once.

Pass Through - Pass Through is a credential function that allows Users to pass through doors that are in secured lockout mode. It does not matter if this mode was set by a door Holiday, or by a Freeze credential used when the door was secured. A Pass Through credential will open the door for the specified relock time.

Dogged - Dogged has only a special function on electronic dogging bars. On these exit bars it keeps the push pad pushed in and the door unlocked. Dogged works as Normal function on all other devices.

Supervised - Supervised credentials follow the "two person rule" Two supervised credentials must be used within five seconds to open the door. The door stays open until the Relock Delay ends.

Prohibit Access (with Alarm) - Prohibit Access (with Alarm) is a credential function that will not allow the credential to open a door, but it will register when the User of this credential tries to do so. It always generates an Audit Event, and additionally sounds the Alarm when the door is equipped with a horn.

CT Aux - This credential function operates only the Auxiliary relay of CT Controllers, but not the Main relay. The time span the relay is activated is specified by the Relock Delay.

CT Main and Aux - This credential function operates both the Auxiliary relay and main relay of Controllers. The time span the relays are activated is specified by the relock delay.

- d) **Badge Layout** - Select a layout for the badge. This is the layout the badge uses when previewed or printed.

Note: This field is enabled only for card technologies. This is not a required field. This dialog follows cardholder field security permissions. If the user does not have at least read only rights to a field, it will not be visible. The user must have read/write permissions to all required fields in order to save a record.

Automatically create CM lock credential

The Schlage system allows the users to automatically create a corresponding offline credential when a new online credential is created.

Follow these instructions to generate an offline credential.

- 1 Open **System Settings** program. Enable **Offline Credential Settings>Automatically create an offline credential when an online credential is created** checkbox.

Note: Only users with administrator rights to System Settings will be able to modify this field because it is a global setting throughout the system.

- 2 Create a new online credential with an Encoded ID. Keypad ID is optional. This feature will not work with credentials created with no Encoded ID. Save the record.

- 3 The application then verifies that the same cardholder does not already have an offline credential with the same Encoded ID and Keypad ID. If the user already has an offline badge that meets these criteria, then the process stops there. The system does not generate any error message.

If the cardholder does not already have an offline credential with same encoded ID and Keypad ID and, an error occurs during the process, the user will be notified of this error with a message dialog. The offline credentials grid will be refreshed and the new credential will be visible.

Note: If Issue Code is in use by the online credential then it must be supported by the offline credential. If it is not, then an offline credential will not be created and the user will be notified via an error message.

Editing CM lock credentials

If you want to modify the offline credentials you have created, double click on the record to open it. Make the necessary modifications and select **Save and Close**.

The system allows users to edit encoded ID and raw data for iButton, PIN, Proximity and Magstripe credentials. Also, when applicable, the system allows users to edit both keypad ID and issue code. Offline access is linked to a credential, not a cardholder. When an offline credential is retired, all offline access records are deleted. By being able to edit the raw data, encoded ID, keypad ID and the issue code the user can now replace a credential without reprogramming access entirely.

Exporting data

- 1 To export the offline credential data to a directory in your hard drive, select the record, and right click on it.
- 2 Select the option **Export Data or Export** and Open Data.
- 3 Choose the directory where you want to export the data.
- 4 Choose the correct format you want to save the data. Available formats: .xml, .html, .txt, .csv (comma separated value).

- 5 Give a file name. Click **Save**.

Deleting Offline Lock Access

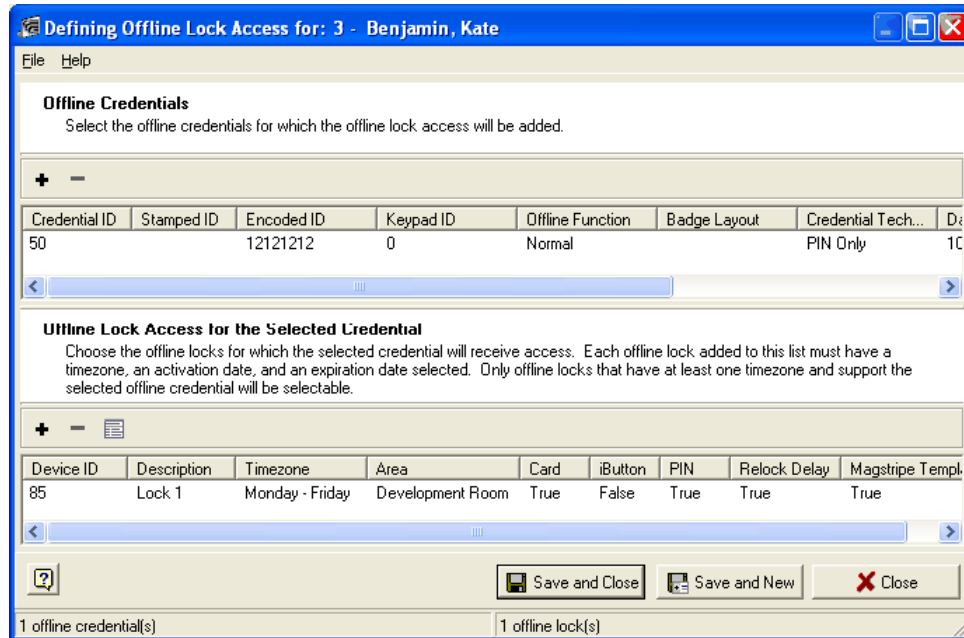
Note: This option applies only to the CM Lock credentials. Campus lock access privileges are defined using the **Campus Lock Access Definition** dialogue.

The next step is defining the access privileges for the offline credentials you created. Follow these instructions to define offline lock access for credentials.

The screenshot shows the 'Cardholder Definition' window with the 'Offline Lock Access' tab selected. The window has a menu bar (File, Edit, Search, View, Tools, Preferences, Help) and a toolbar with buttons for 'New Cardholder' and 'Delete Current Cardholder'. The main form contains fields for 'Activation Date' (3/ 1/2007), 'Expiration Date' (12/31/2199), and 'Cardholder ID' (4). There are checkboxes for 'Access Blocked' (unchecked), 'Controlled Antipassback' (checked), and 'Special Access Privileges' (unchecked). Below these are 'Image Capture Date (UTC)' (4/ 4/2007) and 'Signature Capture Date (UTC)' (6:03:28 PM). The bottom section has tabs for 'Online Credentials', 'Offline Credentials', 'Retired Credentials', 'Area Access', 'Offline Lock Access', 'Categories', and 'E-Mail'. The 'Offline Lock Access' tab is active, showing a table with columns 'Encoded ID', 'Keypad ID', 'Offline Function', and 'Off'. The table is currently empty. To the right of the table is a 'Portrait' photo placeholder and a 'Signature' line. At the bottom left, it says '0 Offline Lock Access Records'.

- 1 Select the tab **Offline Lock Access>Add Offline Lock Access** or select **File>Offline Lock Access>Add Offline Lock Access**.

- 2 Click the + (insert) sign on the upper part of the Define Offline Access for... window.



- 3 Select the credentials that require access to a specific area. The Insert button (+) opens the search window allowing users to select any of the current cardholder's offline credentials. The user can add multiple credentials to the list. But the offline access cannot be given to more than one credential at a time. The user has to select one credential from the list and then define the offline lock access. The system allows users to create multiple access records for a selected credential.

Note: The selected credentials displays in bold characters.

- 4 Once the credential has been selected, the user can use the bottom pane to select the locks to add access. The insert button in the bottom pane brings up the **Offline Lock Access Definition** dialog. Click the insert button to select locks. The system allows the user to select multiple locks for one credential. While selecting the locks, the locks that do not have the selected timezone attached to it display in red and that lock will not be added to the list.

The system does not allow you to mix Magstripe and Proximity credential technologies on the same lock. If a lock supports only Magstripe credentials, you cannot add a Proximity credential to that lock. For more information about this refer to System Manager>Hardware Definitions>CM Lock Definition section.

- 5 Select the + (insert) sign to add the locks. As mentioned above, only locks that have the selected time zone will be available for selection. At least 1 lock must be selected before saving. The user can add the same locks to the same credentials as long as the time zone is different.
- 6 Next click the expand button and select a time zone. This is a required field. Lock that do not have the selected timezone attached to it display in red.
- 7 Now select the activation and expiration dates by using the down arrow located near the corresponding fields.
- 8 Select the **Save and Close** to save the record.

Note: An offline lock can only support 1000 access records.

- 9 Click the **Delete** button in the bottom pane to remove the selected locks from the list view for the selected credential. The edit button in the bottom pane brings up the **Offline Lock Access Definition** dialog in edit mode with the current access record.

Campus Lock Credential Definition

Unlike CM Locks, Campus Locks are assigned by generating credential data which is encoded on Magstripe card. Access assignments are therefore tied to the Magstripe card and the system requires the Magstripe card to be presented for encoding.

Follow these steps to assign a Campus Lock Credential to a cardholder.

Details

- 1 Select the **Offline Credential** tab. Now choose, **Add Campus Lock Credential** button. In the **Campus Lock Credential Definition** window, the **Details** tab displays the following fields.

The screenshot shows the 'Campus Lock Credential Definition' window with the 'Details' tab selected. The window has a menu bar with 'File', 'Badge', and 'Help'. Below the menu bar are tabs: 'Details', 'CAVs', 'Replacement Credential', 'Temp Credential', 'Room Change', and 'Void Credential'. The 'Details' tab contains the following fields:

- Activation:** A date field showing '7/ 5/2007' with a dropdown arrow.
- Expiration:** A date field showing '7/ 5/2008' with a dropdown arrow.
- Offline Function:** A text field showing 'Normal' with a green ellipsis button.
- User Type:** A text field showing 'Maintenance' with a green ellipsis button.
- PIN Requirement:** A text field showing 'Always' with a green ellipsis button.
- PIN:** A text field showing '8076' with a green ellipsis button and a lock icon.
- Gender:** A text field showing 'Male' with a green ellipsis button.
- Badge Layout:** A text field showing 'IR Layout' with a green ellipsis button.
- Stamped ID:** A text field showing '2345' with a lock icon.
- ADA Relock Delay (Seconds):** A text field showing '2' with a lock icon.
- Last Encode Date:** A green bar showing '7/5/2007 5:14:45 AM'.

At the bottom of the window are four buttons: 'Encode', 'Save and Close', 'Save and New', and 'Close'.

- a) **Activation** - Select a date that the credential will start providing access to the selected locks.
- b) **Expiration** - Click the drop down arrow to select the expiration date for the credential. The cardholder's access rights expire on this date. This must be at least one day greater than the activation date. The time the access expires can be changed in the Campus Lock Definition window in System Manager.

- c) **Offline Function** - Offline function specifies the behavior of the Campus Lock Credential. Generally, the selection in Function is the only place to specify Campus Credential behavior, but there is one exception. Campus Locks can be configured to allow Campus Credential with "Normal" function to toggle the lock open or close when swiping the card twice. Click on the expand button to see the list with all functions. Select the desired function by clicking on the function name in the list. The list closes and the new selection appears in the text field of function.
- d) **User Type** - Select a user type this credential is part of. All the enabled user types will be shown in the list. Select the desired user type by clicking on the label in the list. The list closes and the new selection appears in the text field of User Type.
- e) **PIN Requirement** - PIN Requirement specifies whether a PIN is also required while presenting a card to gain access. The mandatory use of a PIN can be enforced for all times, can be required during a Timezone that is assigned to a User Type, or can be never used. Accordingly, the available options in PIN Requirement are "As Defined by TimeZone", "Always", and "Never". Click on to see the list with the options and select the desired option by clicking on the specific entry. The list closes and the new selection appears in the text field of PIN Requirement.

Note: When setting up Timezones that require PIN use, make sure that this Timezone includes all times during which a user type is supposed to have access to that lock. In order for users to be allowed to access a campus lock without mandatory PIN entry during some times, and with mandatory PIN entry during other times, multiple Timezones need to be set up in Timezone Definitions.

Example: All Users with user type "Administration" are allowed to access a lock between 8 AM and 6 PM without entering a PIN. During the time spans 6 AM to 8 AM and 6 PM to 8 PM a PIN entry is mandatory. Between 8 PM and 6 AM any user with user type "Administration" is not allowed to access the lock. This setup requires three TimeZones to be set up.

- f) **PIN** - The Pin value can be automatically generated (a random number) by enabling the option Automatic PIN Length in System Settings>Campus Lock Settings section. You can also enter this value manually. The credential will use this value after it is swiped at a campus lock. This is required field if the PIN Requirement is set to Always or As Defined by lock timezone. If the PIN Requirement is set to Never, this value need not be entered.
- g) **Gender** - Campus locks can be set to allow access rights for male or female users only, or to conduct no check on gender. Click on to see the list with the options "Male", "Female", and "All" and "Other". Setting Gender to "Male" allows access rights to locks that are set to "Male" or "All", setting Gender to "Female" allows access rights to locks that are set to "Female" or "All", and "Other" allows Access Rights to locks that are set to "Other" or do not check gender access. Choose the desired setting by clicking on the list entry. After the selection is completed the list closes and the new selection appears in the text field of Gender.

All means this credential can access all locks no matter what gender access is checked.

Male means this credential can only access locks that have male access only or that do not check gender access.

Female means this credential can only access locks that have female access only or that do not check gender access.

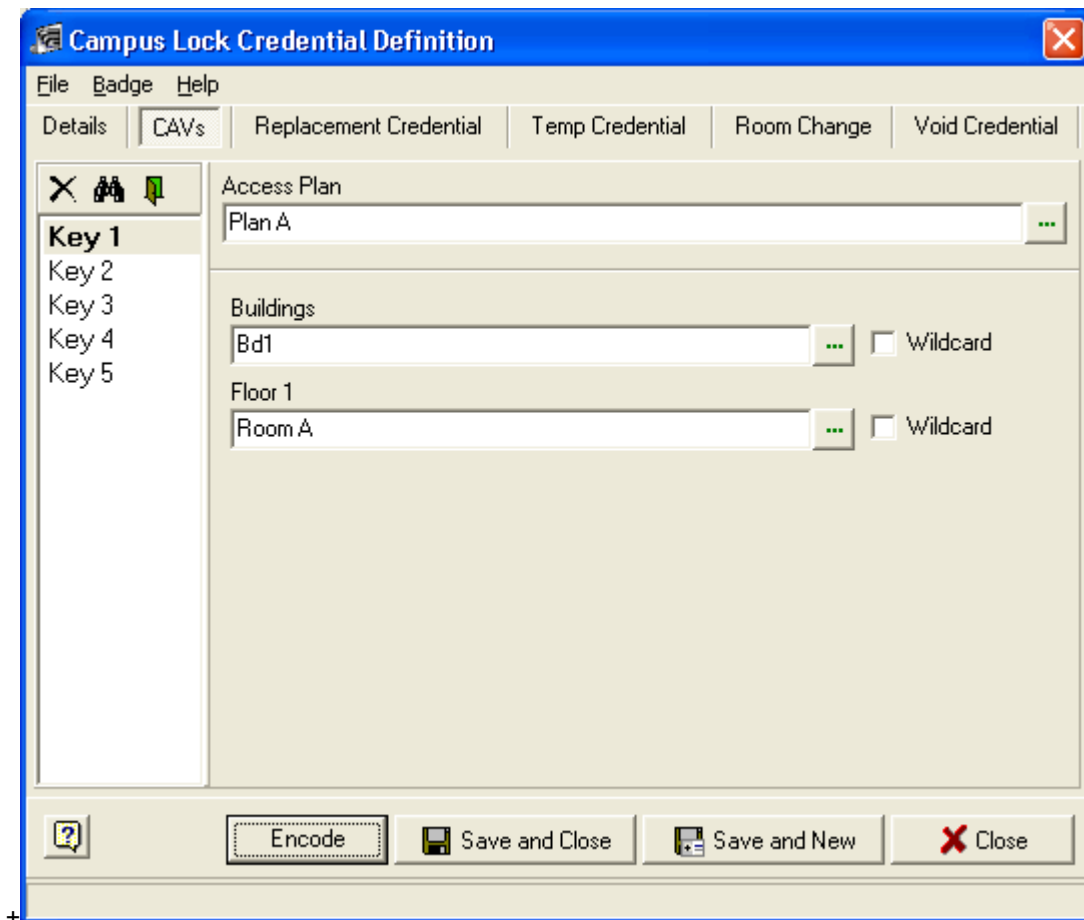
Other means this credential can only access locks that have Other access only or that do not check gender access.

- h) **Badge Layout** - Select a badge layout of the credential. Click on the expand button to see all the defined badge layouts. Select a layout and the list closes. The selected layout will be displayed in the Badge Layout field.
- i) **Stamped ID** - Enter the ID number printed on the badge. This allows the user to distinguish between different credential just by looking at the credential. This must be between zero (0) and 2,147,483,646.

- j) **ADA Relock Delay** - An individual ADA Relock Delay can be assigned to each Campus Lock Credential. The ADA Relock Delay of a credential always overrides the standard Relock Delay time configured for a lock. It further enables the ADA Relock Delay function of a Campus Lock. When both Campus Lock Credential and Campus Lock have an ADA Relock Delay specified, the longer delay time of both will apply, even when it is shorter than the standard Relock Delay of the lock. Enter the delay time in seconds into the text field of ADA Relock Delay (Sec.) or use to increase or decrease the delay time. The default entry is "0" and the maximum amount is 255 seconds.
- k) **Last Encode Date** – This displays the last time the credential was encoded. This is a read only field.

Card Access Values

- 1 Next step is selecting the access plan that this credential will have access. Select the CAVs (Card Access Values) tab. This tab is used to setup the card access value keys for the credential. Access to a particular building, floor or room is given by associating its value to a key. A credential is allowed to have a maximum of five normal keys and one key that will expire on a set date. Multiple keys may be needed for the credential to have access to all the doors. The left part of the tab shows the five (5) keys. Captions that are bold mean that a key is currently defined for that key. When a key is selected, the right part of the tab shows the access plan and the values that the key is currently using. The new access right assignment will not take effect unless the credential is encoded.
- 2 To assign a key, first select a key and select an access plan that is already defined in the system. To assign a key, you need to have at least one access plan defined.



- 3 When a plan is selected, the system displays all the properties and values associated with that particular plan. The controls that you see on this screen depend heavily upon the access plan properties and values defined using the **Access Plan Definition** program. This means that the names shown may be different for each access plan. The property values can be selected by clicking on the expand button next to each property. When you click on the button, the corresponding property values are displayed. The user then must select a value for each property or select the Wild card checkbox which makes it a wildcard. All properties must completely be entered or the key will be invalid and the credential cannot be saved. The delete button above the keys will clear the selected key.

Note: At least one key must be defined to save the credential. Each key can have a separate access plan if wanted.

Any change to a Campus lock credential is only submitted to the database after the credential tied to the currently opened credential record is encoded with updated information. Clicking Encode will first initialize the Card Encoder connected to the PC. A message text appears in red font above the button bar of Campus Lock Credential Definition dialogue. Once the initialization is completed the card encoder is set to write mode and is ready to encode the Campus lock credential. Insert a card into the card encoder when the read/write light of the encoder turns on. A message indicates that the card is successfully encoded.

Replacement Credential

Schlage SMS provides a functionality to limit the damage resulting from a lost Campus lock credential. This tab will only display after the credential has been encoded once and the credential is being edited. It allows the operator to replace a lost credential. The **Encode Replacement Card** button will increment the issue code by one and then encode the new card. The new issue code will only be saved if the encoding process is successful. The new card must be swiped once to disable the lost one. This issue code cannot be manually changed. This system just uses the next value. The first time a card is encoded, the issue code is zero.

The screenshot shows a software window titled "Campus Lock Credential Definition" with a standard Windows-style title bar (blue with a red close button). Below the title bar is a menu bar with "File", "Badge", and "Help". A tabbed interface is present with five tabs: "Details", "CAVs", "Replacement Credential" (which is the active tab), "Temp Credential", and "Room Change". The "Replacement Credential" tab contains two text input fields. The first is labeled "Replacement Credential Stamped ID" and contains a blue cursor. The second is labeled "Issue Code (Automatically Set By System)" and contains the number "0". Both fields have a small icon with a double-headed arrow to their right. Below these fields is a button labeled "Encode Replacement Credential". At the bottom of the window is a toolbar with four buttons: a help icon (question mark in a square), "Encode", "Save and Close" (with a floppy disk icon), and "Save and New" (with a document icon). A red "X" icon is also present next to the "Close" label.

Also the user needs to enter the Stamped ID for the replacement card that is printed on the new card. This replaces the old stamped ID that is in the database.

Temporary Credential

This tab will only display after the credential has been encoded once and the credential is being edited. This allows the operator to issue a temporary card to a cardholder. If the card is completely lost, the Replacement Credential option should be used instead. The maximum expiration date can be set using the System Settings application. The default is seven days. This means that the longest this card can last is seven days from the current day. The activation must be the current day or above and must be one day below the expiration date. The **Encode Temporary Card** button encodes the temporary card using the dates selected.

The screenshot shows a software window titled "Campus Lock Credential Definition" with a standard Windows-style title bar (blue with a close button). Below the title bar is a menu bar with "File", "Badge", and "Help". A tabbed interface is present with tabs for "Details", "CAVs", "Replacement Credential", "Temp Credential" (which is selected), "Room Change", and "Void Credential". The "Temp Credential" tab contains two date selection fields: "Activation" and "Expiration". The "Activation" field shows "7/ 5/2007" and the "Expiration" field shows "7/ 6/2007". Below these fields is a button labeled "Encode Temporary Credential". At the bottom of the window is a toolbar with four buttons: a help icon (question mark), "Encode", "Save and Close" (with a floppy disk icon), and "Save and New" (with a floppy disk icon). A "Close" button with a red X icon is also visible on the right side of the toolbar.

Room Change

Room Change tab is available when the following conditions are met:

- 1 The credential was encoded at least once,
and
- 2 There is at least one campus lock defined to which the user does not have currently access to,
and
- 3 There is at least one CAV on the credential with no wildcards defined (CAV with a wildcard is not displayed on the "Change Room from" list).

The **Room Change** tab is a simple interface of the expire key feature. While using the Room Change feature, instead of the user selecting an existing key, and converting it to an Expire Key, the user selects the lock they want to expire on a specific date and then can give access to a new lock. The user need to then select the expiration date for the room change.

The screenshot shows the 'Campus Lock Credential Definition' window with the 'Room Change' tab selected. The window has a menu bar with 'File', 'Badge', and 'Help'. Below the menu bar are tabs for 'Details', 'CAVs', 'Replacement Credential', 'Temp Credential', 'Room Change', and 'Void Credential'. The 'Room Change' tab is active, showing three input fields: 'Change Room From' with the value 'lock1', 'To Room' with the value 'lock2', and 'Room Change Expiration Date' with a dropdown menu showing '7/ 6/2007'. Each input field has a green expand button to its right. Below these fields is an 'Apply Room Change' button. At the bottom of the window is a toolbar with buttons for 'Encode', 'Save and Close', 'Save and New', and 'Close'.

- 4 **Change Room From** lists all the Campus locks that are currently assigned to the selected credential. Click on the expand button next to the Change Room From field to see a list of all locks that the cardholder has access to and select the one to change by clicking on the specific entry in the list. The list closes and the new selection appears in the Change Room From field.
- 5 Click **To Room** to give the cardholder access to a new room. Assigning a new lock for a Room Change functions the same way as assigning an additional lock with the exception that only one lock can be created. The **Change Room To** selection window lists only those locks the user currently does not have access.
- 6 The **Room Change Expiration Date** option allows the user to select the expiration for the room change. The minimum date is one day after the current date and the maximum date is one year after the current date. A Room change is typically used to allow a person to move things from one room to the other. In order to prevent this person from keeping access rights to the previous room the Room change expires at a specific date. From that date on access rights to the previous room are dropped and only access rights to the new room are in place. Select the expiration date in Room Change Expiration Date. The default date is always one day after today.

- 7 Once you choose the rooms to change and set the access expiration date to the old room, click on the **Apply Room Change** button. The system now displays the information about the temporary access the cardholder has to his/her previous room and the access expiration date. Click on **Remove Access to Room** button to delete the cardholder's access rights to the previous room.

The screenshot shows the 'Campus Lock Credential Definition' window with the 'Room Change' tab selected. The window has a menu bar with 'File', 'Badge', and 'Help'. Below the menu bar are tabs for 'Details', 'CAVs', 'Replacement Credential', 'Temp Credential', 'Room Change', and 'Void Credential'. The 'Room Change' tab contains the following fields and buttons:

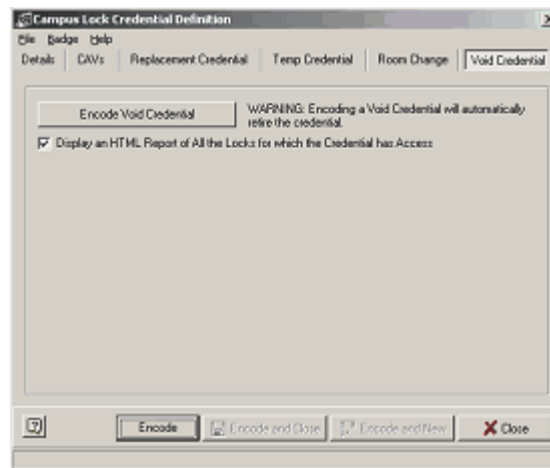
- 'Change Room From' dropdown menu with '<Click to Expand>' and a green expand button.
- 'To Room' dropdown menu with '<Click to Expand>' and a green expand button.
- 'Room Change Expiration Date' dropdown menu showing '7/ 7/2007'.
- 'Apply Room Change' button.
- 'Last Room Change' section containing:
 - 'Room with Temporary Access' text box showing 'lock1'.
 - 'Expiration Date' text box showing '7/7/2007' on a green background.
 - 'Remove Access to Room' button.

At the bottom of the window are four buttons: 'Encode', 'Save and Close', 'Save and New', and 'Close'.

Once all the fields are filled in, the user must use the **Encode** button for the changes to take effect. This saves the record with the room change and then encodes the new credential. The user must present the same card that matches the information in the database.

Void credential

Voiding a credential is an easy way to block a person from accessing the doors that he/she has access. A void credential is created by encoding a card using the information of the credential you want to invalidate. When a void credential is created, the issue code for the credential automatically increments, making the old card invalid. Once a void credential is created, the user must swipe it at all the readers the card had access or reprogram all the locks. When a credential is invalidated, the card is added to the void list.



- 1 **Encode Void Credential** - Put a card into the encoder to create a void credential. Encoding a credential will retire a credential. Once a card is encoded the user can swipe this card on every lock that the person has access. By doing that person's access rights are invalidated.
- 2 **Display an HTML Report of All the Locks for which the Credential has Access** - This option displays a report of all the locks the credential has access. The report will be in HTML format and will launch in the users default browser.
- 3 Insert the card in the encoder and click the **Encode** button. The Retire Credential dialogue is shown. You need to select the status of the credential from the drop down menu and click **Retire Credential**. Now the credential is void and added to the **Retired Credential** list on the main window of the Cardholder Definition.

Automatically generating Credentials

The Cardholder Definition program allows the user to create badges automatically. This feature saves your time because if badge automation feature is enabled in the System Settings, whenever you click **Add Credential** or captures a cardholder image the system generates badges automatically. The user has to create a user-defined field and link it (using UDF LINK program) with the badge technology and the badge layout they will be using in the automatically created badges.

This badge automation functionality works in two different modes.

- 1 **Credential Insert Partial Automation Mode** - In partial automation mode, an online credential is created when the user clicks the Add Credential button.
- 2 **Credential Insert Full Automation Mode** - In full automation mode, an online credential is created only when the cardholder image is taken.

Credential Insert Partial Automation Mode

The following criteria must be met to insert an online credential automatically.

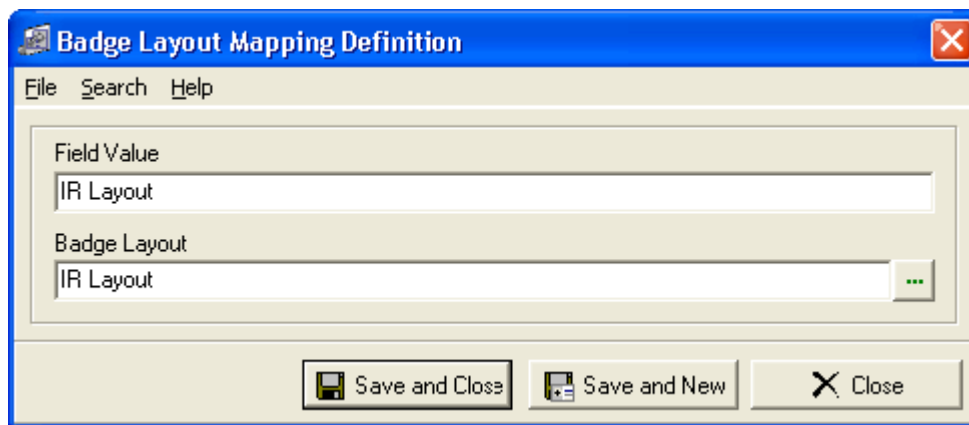
- There should not be an existing blank credential (a blank credential is one without encoded id and stamped id) for the cardholder.
- Valid UDF Cross References must be created for the badge technology and badge layout.

Note: If there is no valid UDF Cross Reference, a dialogue pops up asking you to select the badge layout and badge technology.

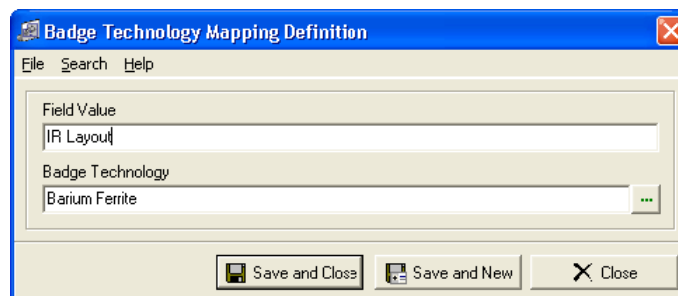
- The user must have at least read only permissions to the cardholder record.
- The user must have at least read/write permissions for badging.
- The option Credential Insert Partial Automation Mode must be selected in the System Settings.
- The option Enter Encoded ID and the Stamped ID Later must be selected in the System Settings

Follow these steps to insert a blank credential:

- 1 Design badge layout and annotations necessary for creating badges.
- 2 Create a user-defined string field that can be duplicated using the UDF Editor. For example create a string field called "Badge Technology Link".
- 3 Using the **UDF Cross Reference** program, link the field you created with a badge layout and a badge technology. In order to do this first, the Badge Layout Mapping must be defined. Assign a logical field value. For this example, "IR - Layout" is typed in the Field Value field. Whenever this value is entered in the relative field in Cardholder Definition, the program will automatically create a badge using the badge layout you have specified here.



- 4 Next define the badge technology mapping.



- 5 Select the user-defined field that you want to use for badge technology mapping. This field is located at the bottom of the UDF Cross Reference window. (You can use the same user defined field that you used for badge layout mapping.)
- 6 In the **System Settings>Online Credential Options and Pin Calculator**, select the following options.
 - Enter Encoded ID and Stamped ID Later
 - Badge Insert Partial Automation Mode
- 7 Click **OK**. If Cardholder Definition program is already open, close the program and open it again.
- 8 Add a new cardholder. In the user defined field that was linked to badge automation, type the same column value that was entered in the Badge Layout Mapping Definition (of UDF Cross Reference). For example, enter "IR Layout". This is the value that was used as our example while mapping the field with badge layout and technology. So whenever you enter the field value of the user-defined field, and click Add Badge button the system will automatically generate a blank badge.

Note: You have to make sure that the UDF you have created is linked properly using the UDF Cross Reference program. Otherwise a dialogue pops up asking you to select the badge layout and badge technology.

- 9 Click **Add Credential**. An online credential is automatically inserted.

Credential Insert Full Automation Mode

When Badge Insert Full Automation Mode is on, badges are generated automatically after the cardholder's photograph is taken for the first time.

The following criteria must be met to insert a blank badge in the Full Automation Mode.

- 1 There must not already be a blank badge (a blank badge is one without Encoded ID and Stamped ID) for the cardholder.
- 2 Valid UDF Links must be predefined for Badge Technology and Badge Layout.
- 3 The user must have at least read only permissions on the cardholder.
- 4 The user must have at least read/write permissions for badging.
- 5 The option Enter Encoded ID and the Stamped ID later must be turned on in the System Settings.
- 6 The option Credential Insert Full Automation Mode must be turned on in the System Settings.
- 7 The Image Date field must be blank.

Now follow steps 1 to 5 in the Badge Insert Partial Automation Section.

Once you have created the user-defined field and linked it with a particular badge technology and badge layout, you can start adding cardholders.

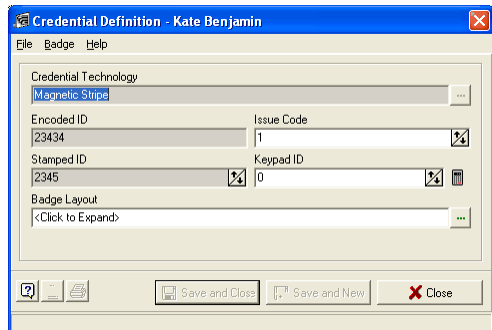
Fill in the required fields. While filling in the user defined field that you used for linking with the badge technology and badge layout, make sure that you are using the same field value that you used for linking.

Note: The field value in **Cardholder Definition** must be the same as the column value that was entered in the **UDF Cross Reference** module.

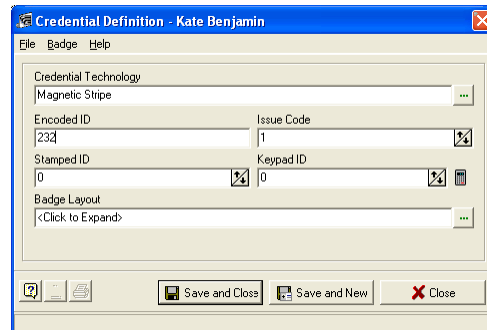
If the system is set to **Badge Insert Full Automation** mode, a blank badge is created when the user captures the photograph of the cardholder for the first time.

Editing Online Credential Information

You can edit an existing credential by double clicking on the badge fields on the main window of Cardholder Definition program. You can change credential technology, badge layout and issue code. If the badge is a blank one you will be able to edit all the fields.



Existing Credential Definition

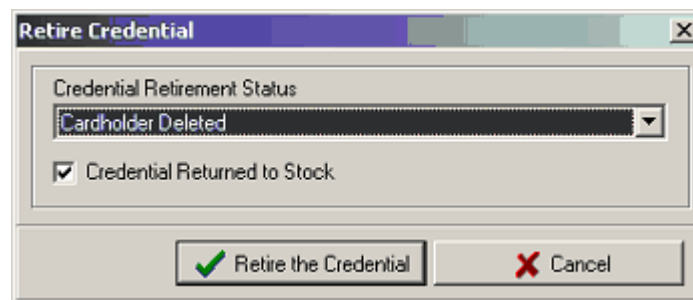


Blank credential definition

Retire Credentials

The **Retire Credentials** button allows the user to retire active credentials whenever they like. This option is particularly useful if a credential is lost or stolen. In such a situation the operator can issue a new credential to the cardholder and retire his/her old credential. This feature helps the users ensure security.

- 1 Select **Active Online Credentials** or **Offline Credentials** tab, highlight the credential that you want to retire. Click the **Retire Credential** button on the tool bar. You can also retire a credential by selecting **File>Active Credential/Offline Credential>Retire Credential** option. The credential no longer has any access control privileges. *(The Encoded ID from this badge may be reused immediately.)* The credential is automatically removed from the **Active Credentials** tab and can be found under the **Retired Credentials** tab. In the **System Settings** program under Badge Options and Pin Calculator section, select "**Retire Active Badges**" option. If you have checked this option, each time you initiate a new badge for the cardholder, a window pops up to select the active badges to retire.



Note: Please note that the lock has to be programmed for any change to take place.

- a) **Credential Retirement Status** - From the drop down menu, select the appropriate status of the credential. The following options are available.
 - **Cardholder Deleted**

- **Lost**
- **Stolen**
- **Destroyed**
- **Suspended**
- **Terminated**
- **Credential Returned to Stock** - Select this option to indicate that the credential is returned to stock and it does not have to be added to the void list.

Note: Void list applies only to Campus lock credentials.

The user can wipe the information on the card and re use it without invalidating the access on that card on every lock.

You can also edit the credentials that are already retired from the Cardholder Definition main window. Select the cardholder record and select the tab **Retired Credential**. Double click on the credential record and the **Retire Credential** window is open. Update the status and click **OK**. **Cancel** aborts the changes you made.

- 2 Select **Reactivate Credential** option to reactivate a retired credential.

Massive access control modification for cardholders

The Cardholder Definition program provides functionality to mass modify Access Control fields of cardholder records (modifying more than one cardholder at a time). The fields you can mass modify are Access Blocked, Activation and Expiration Dates and Controlled Antipassback.

Follow these steps to Mass Modify Access Control fields for more than one cardholder at a time.

- 1 Select **Tools>Modify Access Control** for Cardholders. The following window is displayed.
- 2 Select the cardholder records by clicking **Add Cardholders**. You can use the Search and Advance Search features for adding cardholders. Once you have added the required cardholder records you want to modify, click **Next**.
- 3 In this step you must select the access control fields you want to modify.
 - a) **Access Blocked** - Check the box to enable this field (This sets its value to true.). If you want to block access for the selected cardholders click the box next to the field.
 - b) **Activation Date** - Enable this field by clicking the check box. You can modify the activation date by entering the date manually or click on the drop down arrow to use the calendar. Make sure that the date you enter is a valid date. (It must be the current date or a future date.)
 - c) **Expiration Date** - It works the same way as the activation date. Enable the field and select a valid date.
 - d) **Controlled Antipassback** - Place a check mark in the box next to Controlled Antipassback, if you want to enable this functionality.
- 4 Click the **Next** button to continue. A summary of the modifications you made is displayed. To change any value, click **Back** to return to the previous step. When you are satisfied with the modifications, click the **Finish** button to complete the process.

Add a new Cardholder (Method 2)

- 1 An alternate way to add a cardholder is to fill in the fields on the main window. If you have specified any user defined field as *Required* in the UDF Editor, then a value must be entered in that UDF field as well.
- 2 Click **Save** on the tool bar once you have populated the fields in the top section. After the **Save** button is clicked, the tabs in the lower section of the window become active.
- 3 Enter information for badge, lock access, area access, category and e-mail. Capture an image or signature using the tool bar icons or by accessing them from the View menu bar.

Duplicate Cardholder Information

This function is designed to help you to avoid typing repetitive data for new cardholders. It is useful when you must enter multiple cardholder records that will have the same Area Access and category privileges. It will also replicate user-defined fields that are marked for duplication in the **UDF Editor** module. The default data will appear in the tabs after the required fields are entered. Badge, image and signature information is entered individually for each cardholder record.

- 1 To use the **Duplicate Cardholder** option, first display an existing cardholder record with the same area access and cardholder information or enter a new record with area access and category information that you want to be copied. Now click on the **Duplicate Cardholder** tool bar icon or select it from the File menu.
- 2 Enter the cardholder information in the top section of the screen and click the **Save** icon. Area Access and Category information appears.
- 3 Click the **Active Online Credentials** tab or **Offline Credentials** and choose **Add Online Credentials** (or Offline) to display the **Credential Definition** window. Here you must enter an Encoded ID, Badge Technology and Badge Layout. The Stamped Number and Issue Code are optional fields.
- 4 Next you can capture images and signatures. For pictures, choose the **Capture Image icon** on the main screen tool bar or chose Image from the View menu. The Cardholder Image window is now displayed. Choose your Capture Source then select the Capture button on the bottom left corner. Your cropping options become active on the tool bar and in the Tool menu bar option. When you are satisfied with the image click **OK**.

To open the **Cardholder Signature** window, select the **Capture Signature** icon on the tool bar or choose **Signature** from the **View** menu. This feature works exactly like the **Capture Image** screen.

Adding email addresses

Cardholder's e-mail addresses can be stored in the system. The user can either insert new E-mail addresses or associate the cardholder information with the existing addresses that are stored in the system using E-mail Address Editor application. This option is also equipped with a search feature that allows you to find records easily.

- 1 To add a new e-mail address, select the **E-mail Addresses** option from the lower pane of the window and choose the + (plus) icon.
- 2 On the **Insert E-mail Addresses** window, type in the E-mail address. You can add as many records you want.
- 3 Click **OK**. The records are shown in the **Address** section of the main screen.
- 4 You can also select the existing e-mail addresses and associate with a cardholder information. Select **Associate Existing E-mail**.

- 5 On the Search window, enter the text in the **Search Criteria** field and click **Find Now**. Just clicking the **Find Now** button displays all the records defined in the system. Select the appropriate records and click **OK**.

Deleting email addresses

- 1 If you want to remove an e-mail address from a cardholder record, open the cardholder record and select the E-mail Address tab located in the lower section of the window.
- 2 Select the e-mail address you want to delete and select the delete icon from the tool bar.
- 3 A confirmation message is displayed. Choose **Yes** to continue.

Note: If the e-mail address you are trying to delete is attached to a report (used in the Report Scheduler program) you cannot delete the record. A warning message is displayed preventing you from deleting the record.

Modifying and Deleting Cardholders or Cardholder Information

Cardholder data can be modified and deleted directly from the main screen and by using menu or tool bars. Locate and display the cardholder by using the Search feature. You may type over information in any fields in the top section of the window then use the tabs and the tab tool bars to change badge, area access and category information.

The grids of tabs cannot be modified. The quickest way to modify a field is to click on the record and use the picture icons. To edit a Date field use the drop down arrow to display the calendar or type the change directly in the field. Highlight the year field and right click your mouse to open the shortcut named "Go to today". The field displays the current date.

To delete information on a cardholder, highlight the field within one of the tabs and select the appropriate delete icon from the tab tool bar. To delete a cardholder from the database, search and display the cardholder then chose the Delete Cardholder icon.

Delete Cardholders

The following are the conditions for deleting cardholders.

- 1 The user must have read/write permissions or greater to the cardholder (through category permissions)
- 2 The user must have read/write permissions or greater to Cardholder Definitions (through launcher permissions)
- 3 The user must have read/write permissions or greater to Cardholder ID (through cardholder permissions).

Deleting a single cardholder record

- 1 Using the Cardholder Search wizard, select the cardholder record that you want to remove from the database.
- 2 With the record displayed on the main screen, select **Edit>Delete Current Cardholder** or choose the tool bar icon. A confirmation message is displayed. Click **Yes** to delete the cardholder.

Multiple cardholder deletions

In the Cardholder Search wizard, choose the records to be removed from the database. This feature is separate from the Delete Cardholder icon that resides on the tool bar.

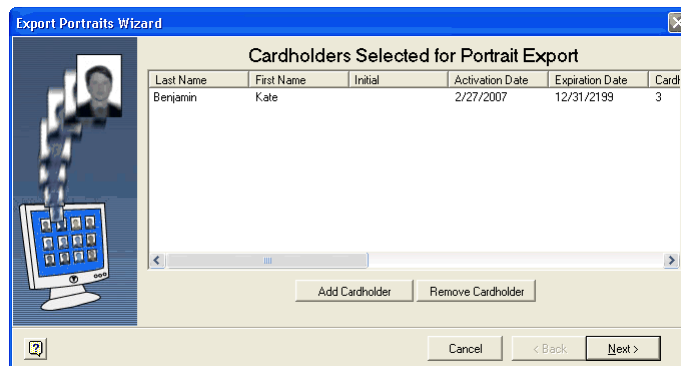
While deleting multiple cardholders at the same time, any attempt that fails will be added to a list view and when the deletion is complete, a dialog pops up with a list of cardholders who were not deleted and showing the cause of the error.

- 1 Select **Edit>Delete Multiple Cardholders** or select the tool bar icon. The Cardholder Search window will display. Use your control (Ctrl) key to make multiple selections. Click **OK**. A confirmation message is displayed to verify the number of cardholders to be deleted. Click **OK**.

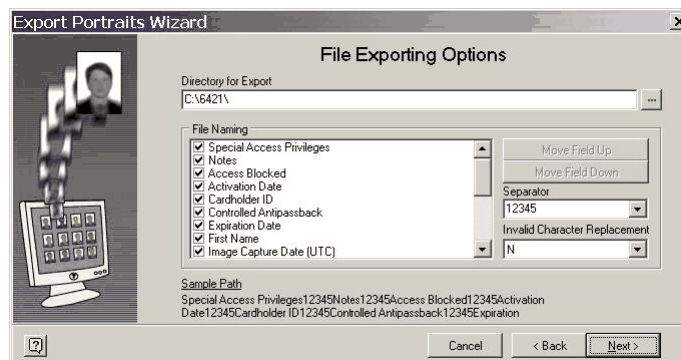
Exporting Cardholder Portraits

This feature provides an **Export Wizard** that sends cardholder images to a separate file. These files can reside on the local drive or can send across the network to and saved on a different computer. This is useful when you want to store image copies on a different server or when a picture needs to be attached to an E-mail message. It is recommended that the file that you want to export reside outside of the **Schlage SMS** software.

- 1 Select **File>Export Cardholder Portraits**. The **Export Wizard** permits you to copy portraits to a new file located outside of **Schlage SMS**. The **Add Cardholder** button links to the Cardholder Search Wizard. Highlight your selections and click **OK**.



- 2 A list displays when a portrait is not be exported. The wizard displays the cardholders selected for export.
- 3 The next step is to select the path, file naming convention and file name separator.



- a) **Directory for Export** - Type the full path or use the Browse button to select your folder location.
 - b) **File Naming** - The Export folder contains the JPG images of your cardholders. Select a good naming convention under the File Name section. When choosing a combination of fields, you can determine the order by using the Field Up and Field Down buttons.
 - c) **Separator** - This is used in conjunction with file names that use several fields.
Example: When using a period, the file name format in the folder will be Last.First.jpg such as Doe.John.jp. A forward slash, back slash or star symbol is not permitted as a Separator. An error message displays if one of these characters are entered.
 - d) **Replacement Character** - Click on the down arrow to select a character that replaces any invalid characters in the file name.
- 4 Click **Next**. A summary of the export is shown in the next window. Click **Finish** to start the export process.

Printing Dossier Reports

A Dossier is a type of Badge Layout that has been identified as such in the Badge Creation module. A Search window allows the user to select from a list and send the report to be printed.

Dossier Reports can be sent to queues just like badges. While printing the reports select the option “*Send Dossier Reports to Printer Queue.*”

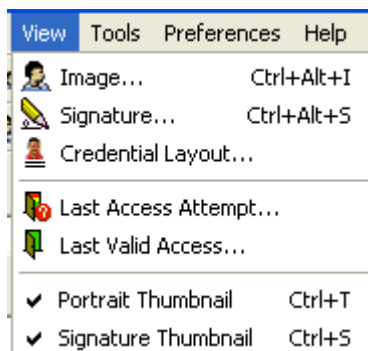
Note: The system will default to the option set in the System Settings program. In the System Settings if you have set the option as “Send Dossier to Default Printer” the system will automatically defaults to that option.

If you have set a default dossier queue in the System Settings the system will default to that dossier queue automatically.

Print Portrait Export Report: This report is created and printed when the user selects the date of the file export.

View

The following are the options available under the **View** menu.



- 1 **Image** - This selection opens the Cardholder Image screen. The user can capture a picture or manipulate the image utilizing the tool bar icons, Crop Rubber band, Crop, Edit and Save. Image settings for this window are enabled in the System Manager Settings module.

Image screen options

- a) **Crop Rubber band** - Selecting this icon activates the red cropping band. Drag the edges of the band to change the area of the picture. (*In the System Settings module, "Allow Crop Rubber band to be Moved or Sized" must be checked to set the value to true.*)
- b) **Crop** - This option will trim the picture to display only what is inside the red cropping band.

Note: All these features are available through the tools menu.

- 2 **Signature** - This feature opens the Signature Image screen. The user can capture a signature or manipulate the image utilizing the crop and edit features. Signature options work like the image screen.
- 3 **Credential Layout** - On the Active Online Credential/Offline Credential tab, highlight a credential then click the Credential Layout icon to view the cardholder's badge.

You can also view the back of the image. Right click on the badge and click on **View Page 2** from the option.



- 4 **Last access attempt** - The **Access Attempt** window provides Transaction, Cardholder and Reader information fields. It displays the last time a cardholder has swiped a card at a reader regardless of whether they were granted or denied access.
- 5 **Last valid access** - This window contains the cardholder's most recent **Valid Access** information such as transaction date and time, cardholder and reader information. This is very useful when you must immediately find a cardholder's last known location.
- 6 **Portrait thumbnail** - If this option is selected the system shows a thumbnail image of the cardholder in the lower pane of the main window of the application.
- 7 **Signature thumbnail** - If this option is selected the system shows a thumbnail image of the signature of the cardholder in the lower pane of the main window of the application.

Cardholder Search

When you click on the binocular icon, the Cardholder Search Wizard is activated. There are three search features. They are Find Cardholder, Find Previous Cardholder and Find Next Cardholder. You can search by Last Name, First Name, Credential Data (Encoded ID, Stamped ID or Raw Card Data) or by User Defined Fields.

Last Name	First Name	Initial	Activation Date	Expiration Date	Cardholder ID	Encoded ID	Access Block	Controller
Benjamin	Kate		2/27/2007	12/31/2199	3	45465465		

To view the entire cardholder database, press the Find Now button without entering a value in any field. *The default search order is displayed alphabetically.* To search by a user-defined field, place a check mark in the UDF Search field and fill in the values.

- 1 **Previous in Search** - This will display the previous cardholder in the database according to the sort order that was selected in the above option.
- 2 **Next in Search** - This will display the next cardholder listed in the database according to the cardholder sort order.
- 3 **Show Results on Load** - This search feature is intended to be used the first time the module is opened. Checking one of the sub-menu items will load all the data when the search form is opened. An unchecked item will display a blank search form and the user must enter values for the search.
- 4 To change the sort order, left click on a column heading. For instance, to sort by Cardholder ID, click on the Cardholder ID title bar. Your sort order directly affects Previous Cardholder in Search and Next Cardholder in Search. Size and order of columns can be changed by dragging and dropping to a new location. The bottom left corner of the screen will display the number of cardholders that have been selected

Advanced find Feature

Using Advanced Find, you can build the search criteria by selecting appropriate entries from the drop down list box and entering specific value in the value field. You have to select a specific field name, condition and a specific search value.

Advanced Find feature uses Boolean logic to create complex and highly precise searches. Boolean logic uses three connecting operators (NOT, AND OR) to narrow or broaden a search or exclude a term from the search. It is the process of linking criteria to narrow or expand a search through the use of **NOT**, **AND** or **OR**.

The Advanced Find feature helps the operator to customize the search function. The operator can define the searches and save them for later use. The saved search criterion is displayed only for the operator who defined it.

Cardholders can be searched using cardholder fields (like first name, last name etc.), badge criteria or activation and expiration date.

- 1 Click on the **Advanced Find** tab located on the top of the Search window.
- 2 The Advance Find of Cardholders window opens.
- 3 Click on the Cardholder Fields button to search for cardholders by field name.
- 4 Define your search criteria.
 - a) If you want to search for Cardholder ID = 10, you need first select the left parenthesis from the list box.
 - b) Parenthesis can be used to create nested search clauses. Using the Parenthesis one can override the standard order of priority (left to right) for each Boolean statement in the search.
 - c) Select Cardholder ID as the Field Name.
 - d) Select equal to (=) as the condition.
 - e) Enter the value as 10.
 - f) Provide the closing parenthesis at the end.
 - g) When you are satisfied with the criterion, click **Add to List** button. If the criterion is not valid, it is displayed in red under the Where Clause section. When the criteria becomes valid the font color changes to black.
 - h) If you would like to specify additional search condition you can select AND/OR from the list box.
- 5 E.g. If you want to search Cardholder IDs less than or equal to 10 and last names with the letter "K" and Cardholder IDs greater than or equal to 20 and last names with the letter "D", define the search criteria as follows.

((Cardholder ID>=10) AND (Last Name Like d%)) OR ((Cardholder ID>=20) AND (Last Name LIKE%d%))

Advanced Find of Cardholders

File

Search For Cardholders

Cardholder Fields | Credential Criteria | Activation and Expiration | Area Access | Categories

Find items that match these criteria:

NOT	(Field Name	Condition	Value)	AND/OR
	(Cardholder ID	<>	10)	
	(Last Name	LIKE	Benjamin)	

Where Clause
 ([Cardholder ID] <> 10) ([Last Name] LIKE Benjamin)

Edit Remove

Define Criteria

Not (Field Name Condition Value) AND / OR

☐ (Access Blocked = True)

+ Add To List

Find Now
New Search
Cancel

- 6 When you run the search you will get the records corresponding to your search criteria. The following window shows the search result.
- 7 Once you have defined the criteria click **File>Save**.
- 8 Add a description to your search and click **OK**.
- 9 The new search is saved for future use and listed under the **Advanced Find** button.
- 10 You can also search for cardholders using Badge Criteria, Activation and Expiration Date, Area Access and Categories.

Use of wildcard

The Advanced Search feature provides ways to select certain cardholder records without typing complete information. Schlage System allows the use of wildcard (more formally known as *metacharacters*) to stand for one or more characters in a cardholder record. A wild card is a value entered into a query field that represents any other value and is usually used when exact values are not known. The users can do partial match searches by using the% (percent sign) as a **wildcard**. Within the search criteria, a user can type the% character before or after their search text as a wildcard.

E.g. Entering%*er* will return all the last names that end with the letters “*er*”. By using the wildcard in the beginning, the user is requesting the system to find all parts that ends with “*er*” and could have additional characters in the beginning.

Berner

Creager

Kaiser

Entering%*er*% will return all the last names that contain the letters “*er*”.

Anderson

Berner

Creager

Kaiser

Roberts

Slathers

Wildcard has a very flexible capability to help users identify specific information based on limited or partial search information. One thing to note; however, this capability can result in very large query results if misused.

Exporting Search Results

Cardholder search results can be exported to your hard drive in the following formats:.xml,.html,.txt,.csv (comma separated value).

To export search results to your hard drive,

- 1 Run a search and right click on the search results.
- 2 Click the **Export Results** button.
- 3 Choose the directory to which you want to save the results. Give a file name. Click the drop down menu to choose an available file format.
- 4 Click **Save** button to complete the action and the search results will be saved in your system.

Note: Exporting Cardholder Search Results feature is also available in the **All Cardholders** tab in the System Manager module.

You can also search for cardholders based on their area access.

- 5 Select the **Area Access** tab on the **Advance Find** window.

- 6 Select the Areas to which the cardholders you want to find have access by clicking on the **Add Areas** button. You can run a search to find the areas easily. Select the areas and click **O.K.**
- 7 Click the **Find Now** button in the **Advanced Find for Cardholders** window.
- 8 The search results are displayed in the **Search** window.

Credential criteria

Advanced Find of Cardholders

Search For Cardholders

Cardholder Fields | **Credential Criteria** | Activation and Expiration | Area Access | Categories

1) First select the search type. 2) Next select the range for the search.

☒ **Credential ID** Beginning ID To Ending ID (Blank searches on Beginning ID only)

☐ Encoded ID ☐ Stamped ID ☐ Raw Card Data

☐ Created Between

5/25/2007 12:00:00 AM
And
5/25/2007 11:59:59 PM

☐ Printed Between

5/25/2007 12:00:00 AM
And
5/25/2007 11:59:59 PM

☐ Include Retired Credential
☐ Find All Cardholders with no Credentials

Find Now New Search Cancel

- 1 First click on the Credential Criteria tab. Select the search type. Search by **Credential ID**, **Encoded ID**, **Stamped ID**, **Raw Card Data** or credential creation dates by clicking the appropriate radio button and entering the information.
- 2 When a search is run by **Badge ID**, **Encoded ID** or **Stamped ID**, you can select a range between the **Beginning ID** number and **Ending ID** number.
- 3 For example, if you would like to search for all cardholders that have been issued badges for the last seven days, click **Creation Between** and use the calendar drop down to select the dates.
- 4 You can retrieve the credential information by connecting Schlage Enrollment Reader to the PC where the **Schlage SMS** is running. You can extract information from Magstripe, Proximity and iButton credentials.
- 5 The **Auto Retrieve** option next to the Encoded ID box allows to retrieve Encoded IDs using the following credential technologies; Magnetic Stripe, Proximity, and iButton. The user must select one of the options from the drop down menu and then present the credential to the CM Lock or CIP connected to the computer. The Encoded ID can be automatically retrieved only from CM Lock Credentials. The user can search for Encoded IDs between 0 and 4294967295.
- 6 Campus Lock Credentials can be automatically retrieved using the Credential ID search type. First select the **Credential ID**, then select the **Campus Lock Magnetic Stripe** menu option under the **Auto Retrieve** button. This prompts you to place the card in the encoder. Once the card is read, the **Beginning ID** field is automatically filled in. The Ending ID field will be blank. Click the Search button to complete the search.

Note: The **Campus Lock Credentials** cannot be automatically retrieved from the lock itself. You need an encoder to retrieve the credential ID.

- 7 The **COM Port** and **Time-out** are the same settings that are used when adding CM lock credentials and using the Auto Retrieve button (System Settings>Campus Lock Settings>Current Workstation Settings).
- 8 Another option is to run the search based on the credential creation dates or credential printed dates. Select the appropriate option and enter the dates and time.
- 9 Click the **Find Now** button to initiate the search. You can also search for badges that have neither Encoded ID nor Stamped ID (blank badge). For example, place a check mark next to Encoded ID. Next, check the box *Selection is not currently defined and* run the search. You can see that all the badges that don't have Encoded ID are displayed.
- 10 You can also check the option to **Include Retired Credential** and **Find All Cardholders with no Credential**.

Categories

Follow the same procedures described above to search for cardholders based on their categories. Instead of Area Access select the **Categories** tab, and add categories.

Selecting a Cardholder

Highlight a cardholder and select the **OK** button. The application returns you to the main window and displays the cardholder's information. Once a cardholder is open in the main window, the **Find Previous Cardholder** and **Find Next Cardholder** icons become active. The Previous and Next search are based on the current sort order.

Card Format Editor

CHAPTER 6

Introduction

The **Card Format Editor** allows the user to create a new credential format, modify an existing credential format or select a previously defined card format. The system supports the following credential formats:

- **Magstripe format**
- **Wiegand format (for proximity credentials)**

A user created credential format will be saved with the next available Card format ID in the range of 2000 - 3000. All the card formats below this range are factory set and cannot be modified. To set up a format, the user can either read the card using an enrollment reader or enter the raw data directly into the field. The user can specify positions of encoded ID, site code, and issue code. The "Show Sample" button allows the user to view the encoded ID, site code, and issue code from the raw data.

Accessing the application

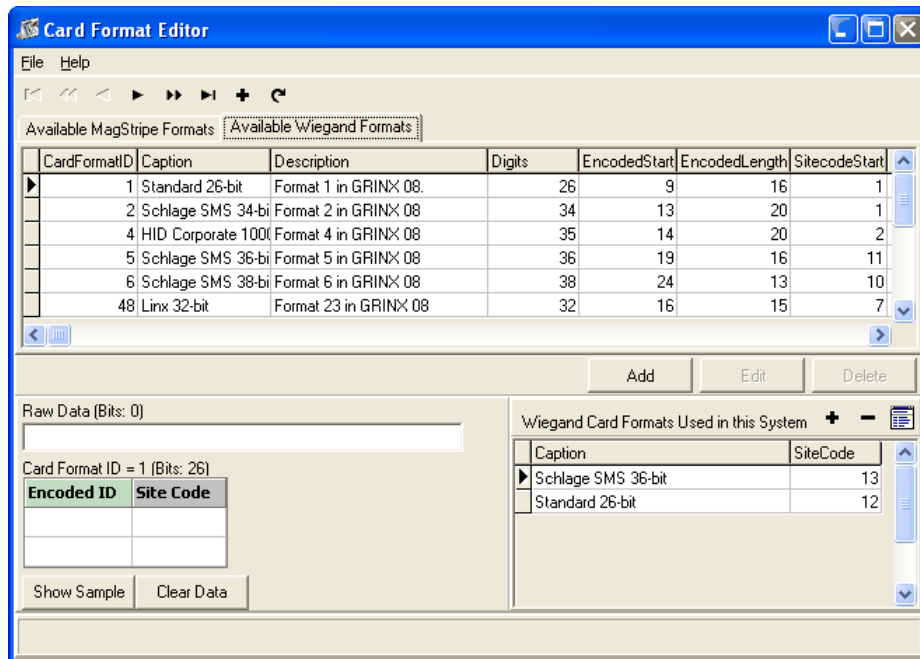
- 1 Go to **Start>Programs>Schlage SMS>Schlage SMS** or double click on the **Schlage SMS** icon from the desktop.
- 2 In the **System Launcher**, double click on the **Card Format Editor** icon.

Overview

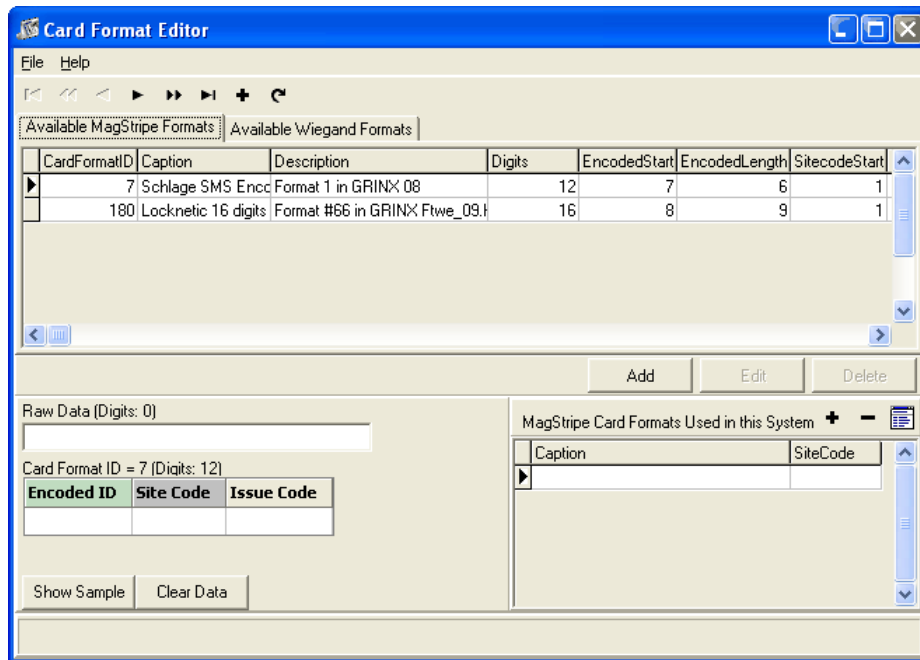
Card formats are used to split up the data on a credential for use at either online or offline devices. Formats are simply patterns that specify which numbers are grouped together, and the purpose of each group. As an example the numeric string 3141592653 might refer to a phone number and be written (314) 159-2653 where 314 is the area code, 159 is the exchange and 2653 is the specific phone. If you look it up on the Internet, at least one person claims it as his fax number. If you dial it, however, you will get a message saying that it is an invalid number, which make sense since no exchange ever begins with the number 1. Actually, it is written 3.141592653 which is the ratio of a circle's circumference to its diameter (π) computed to the first 10 significant digits. Another example is 206250141 which could be a ZIP code (20625-0141), a Social Security Number (206-25-0141) or an Employee Identification Number (20-6250141). Note how similar the pattern and notation are among these three different formats with very different purposes. As a ZIP code, the second group can refer to a single box number if 20625 is a small post office, or to a group of boxes or street addresses if the first group refers to a post office serving more citizens than Cobb Island, MD does. This example shows that even with well defined formats the purpose can vary based on context. This is why you cannot have more than one format for any given length in use on your system.

Card Format Editor main window

The main grid in the above windows show which formats are available for use in your system. There are two kinds of formats, Wiegand (for proximity badges) and Magstripe (the more frequently seen format, such as driver's licenses, credit cards and hotel key cards). If you prefer a different sort order, simply click on the label at the top of the column which you want to sort, the same way as you do in Windows Explorer.



The smaller grid in the lower right hand corner shows which formats are already specified for use in your particular system (two Magstripe formats in this example). The Card Format ID grid and Raw Data text entry box in the lower left corner are used to create new formats in case your existing credentials are in a nonstandard format. This is where the Enrollment Reader will write the data it reads from a credential.

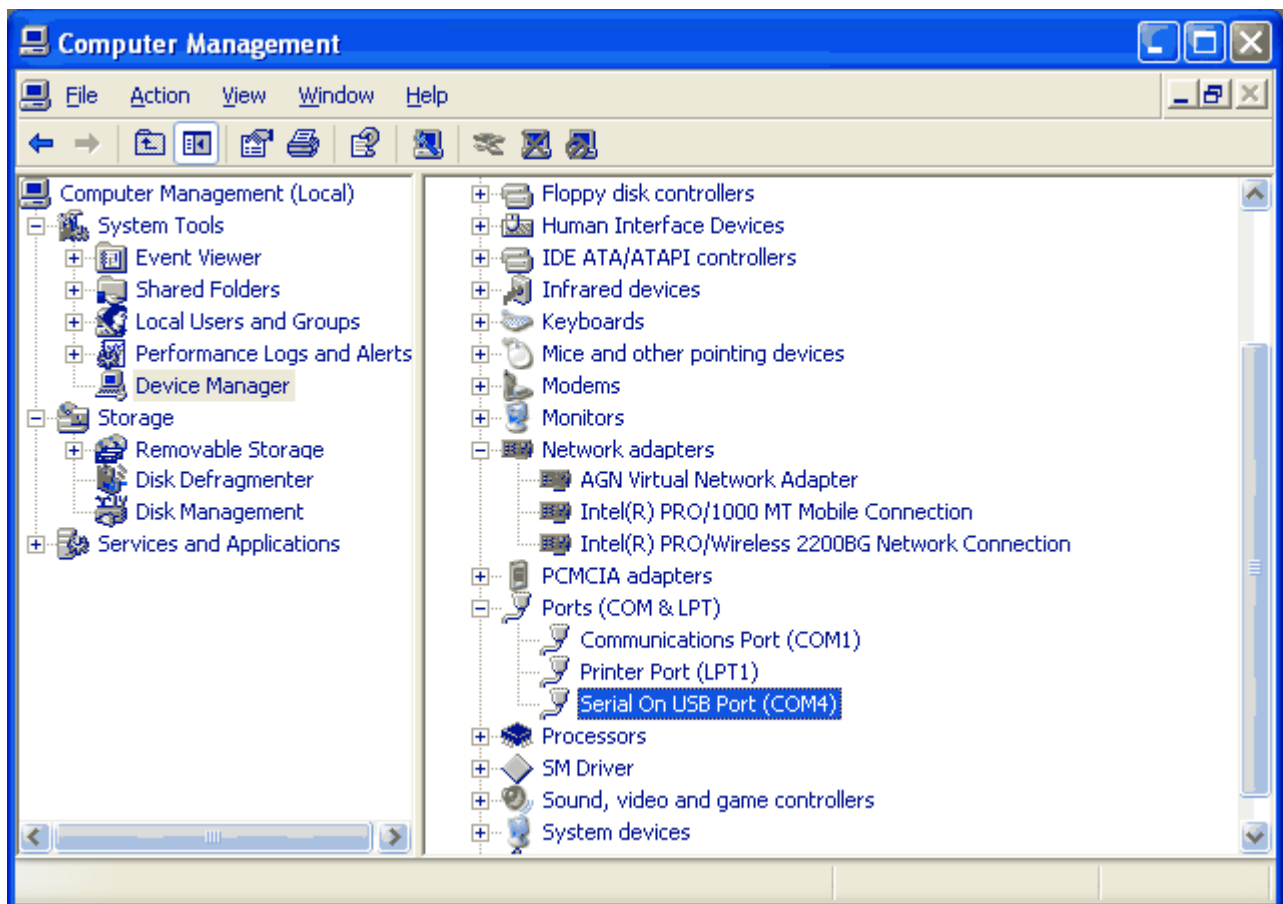


Setting up Schlage Enrollment Reader

The credential data is retrieved using either Schlage Enrollment Reader or Offline Enrollment Reader. This enrollment reader is connected to a PC running the Schlage SMS software via a serial port or via an included serial->USB adapter. To use the USB Port Adapter, you must first install the driver software on your computer. Once the driver has successfully installed, you will need to restart your computer. This device has Magstripe, Proximity, and iButton read heads.

Connecting the hardware and determining the COM Port

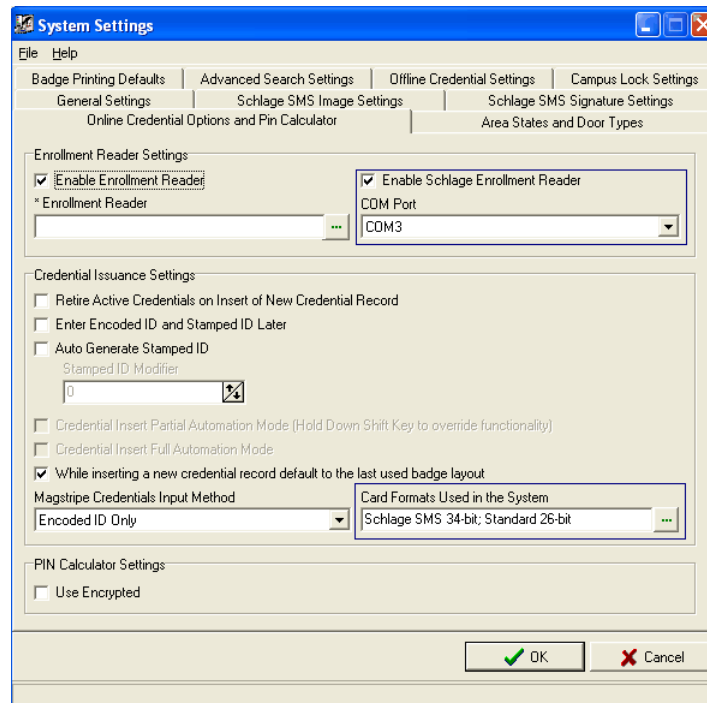
- 1 Connect the USB Adapter to the USB Port of your computer.
- 2 Go to My Computer. Right click on **My Computer**, select **Manage**. This opens the **Computer Management** screen.
- 3 On the Computer Management screen, select **Device Manager>Ports (COM and LPT)>Serial on USB Port (COM #)**. It shows the specific COM Port that is used to connect the Enrollment reader.



Setting up the Enrollment Reader in Schlage SMS

- 1 Open System Settings program. Choose the tab, **Online Credential Options and Pin Calculator**.
- 2 Under the **Enrollment Reader Settings**, select **Enable Schlage Enrollment Reader**.
- 3 Now select the **COM Port** that is used to connect the Enrollment Reader. This Com Port must be the same that you have determined in the previous step.

- 4 In order to add credentials, the system needs to know the format of the credential. Click the browse button near the **Card Formats Used in the System** field. It opens the Card Formats Used in the System window. Choose the card formats that you will be using.



Magstripe Template

Please select **File>Magstripe Template** option to define Magstripe Template. For further information on defining Magstripe Templates refer to **System Manager>Magstripe Template Definition**.

Card Format Editor usage scenarios

Online and offline devices read this data in different ways. Card formats are used to translate between these two views of the data. The offline view of the credential data is called "raw card data"; the online view is called "Encoded ID". You have choices regarding how to enroll credentials based on which scenario applies to your installation.

- 1 **Your entire system uses online locks only** - You might not need to use the Card Format Editor. Credentials can be added by Encoded ID, and raw card data left blank. Standard reader interface and reader controller firmware support these formats. If you want to use the enrollment reader to enroll credentials in Cardholder Definitions, you will need to either choose an existing format or setup a new format for use in the system.

For Wiegand cards

- **Format ID 1:** **Standard 26-bit**
- **Format ID 2:** **Schlage 34-bit**

- **Format ID 4:** **HID 35-bit**
- **Format ID 66:** **Locknetics 37 Bit Wiegand Format**

For Magstripe cards

- **Format ID 7:** **Schlage encoded magcards**
- **Format ID 128:** **Locknetics 16-digit magcards**

For iButtons

- **Format ID 1:** **Locknetics Customer iButton**
- **Format ID 2:** **General iButton**

If your credentials are not in these formats you will need custom firmware on either the reader controller (for wireless and VIP locks directly connected to the controller) or reader interface (for any reader connected through an RI). You may be able to get format information from your credential vendor.

- 2 **Your entire system uses offline locks only** - You might not need to use the Card Format Editor. As long as no card formats are selected under the "selected formats" list, the system can enroll only the raw card data useful for offline locks and leave Encoded ID blank. You may wish to setup a card format anyway, if the credential data is well understood and online devices may be added to the system later. Again, you may be able to get format information from your credential vendor.

- 3 **Your system uses both online and offline** - You should set up a card format. Once this is done correctly, the enrollment reader can extract both the raw card data and Encoded ID from the credential.

If you have only online locks or only offline locks, the simplest method is to present each credential to the Enrollment Reader and use the data as is. Please note that you will still need to specify the format of your credential for the online locks. If your format is not one listed above, you will need to create it using the Card Format Editor.

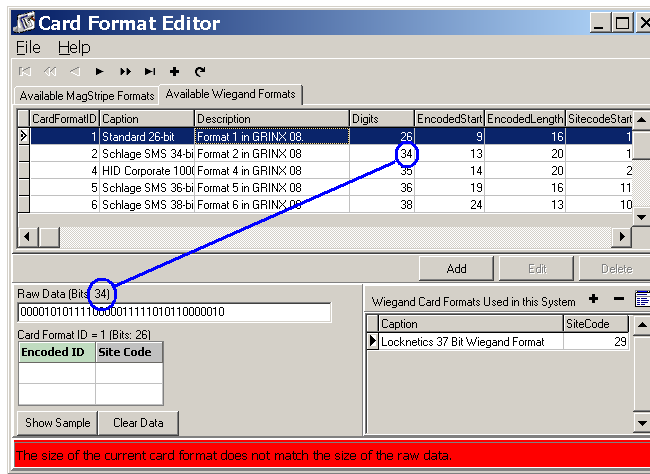
One possible drawback is that all credentials must be entered this way. If you cannot (or prefer not to) present all credentials, or if you need to use both types of locks, you will need to specify which formats are being used. If you buy new badges from a different vendor, you must add their format to the Schlage SMS system. When specifying details for the new vendor, remember that you can have only 1 format of any particular length. This technical requirement may limit your choice of vendors.

Identifying existing credential formats

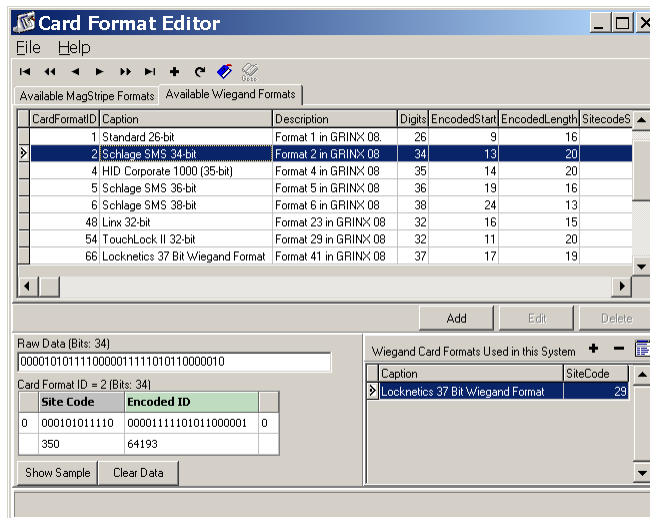
The purpose of the **Card Format Editor**, assisted by the **Enrollment Reader**, is to enable you to identify or define existing credential formats to the system with minimal effort.

- 1 When you present an existing credential, either by running a Magstripe card through the slot or holding a Wiegand card near the proximity sensor, the Card Format Editor will switch to the correct tab (based on credential type). Then the data stored in the credential memory will be sensed and written into the Raw Data edit box. Your task is to figure out which format is in use based on a few indications.
- 2 If your credential does not match the first format, you will see this message at the bottom of the window:

“The size of the current format does not match the size of the raw data.”

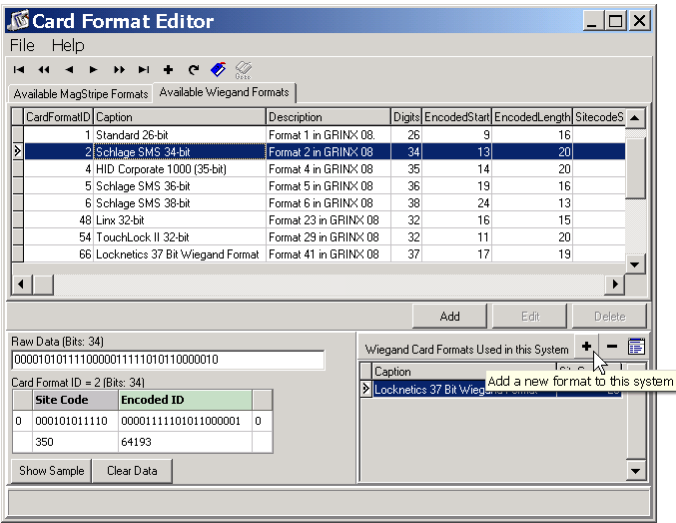


- First try a format which fits the length of your sample data. Just above the Raw Data edit box, the label lists the length (Binary digits, aka Bits for Wiegand and hexadecimal digits for Magstripe). In this case, length is 34, so look at the Digits column to find a format of the proper length. Click on the second line, CardFormatID = 2. This will cause the display in the lower left portion of the window to change as shown below:

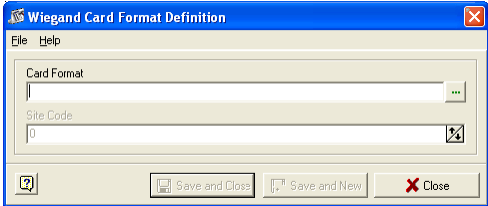


- Look on the credential to see whether there is a number printed on it. If the number matches the Encoded ID, you can be sure this is the right format. If you have more than one format choice for the length of the data (as shown in the Digits column), try them until one matches up this way. You could also enroll several credentials and look for similar numbers in similar places. These would be either the site code or issue code. You should be able to find your site code by contacting the office which generates new credentials. This would be either your vendor or a group in your organization.

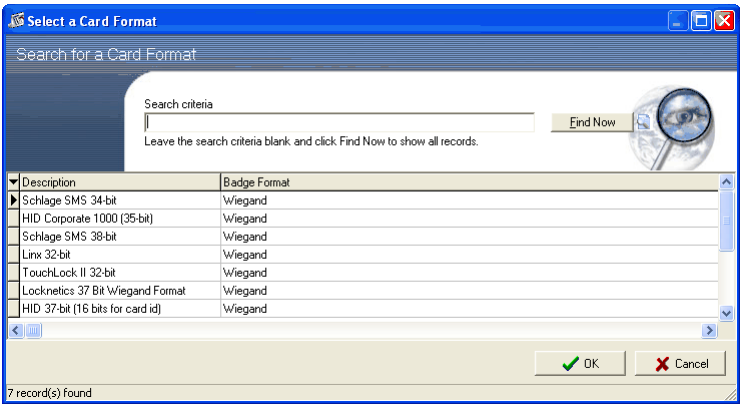
- 5 To add this preset factory format to your specific system, click the small button with a + sign, below the Delete button:



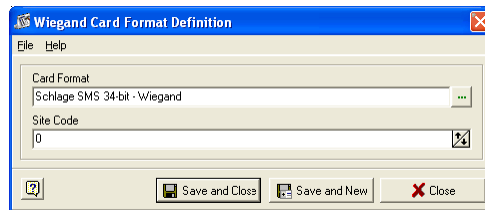
- 6 You will see:



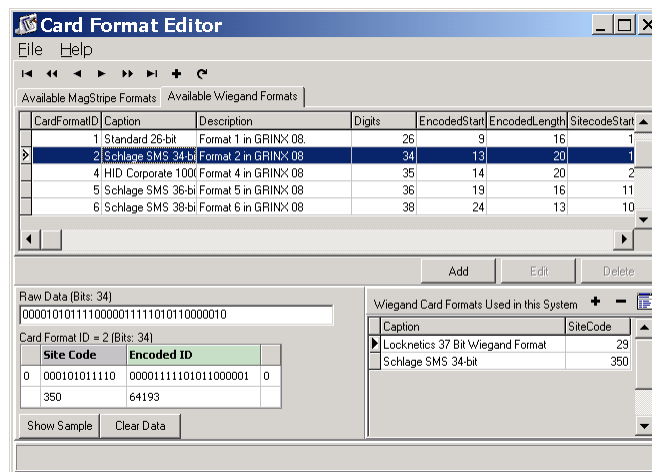
- 7 Click on the browse (three dots) button to the right of the Card Format box. Select the format you found earlier and click the **OK** button.



- 8 You will see:



- 9 Click on the **Site Code** field and enter the **Site Code**, (values between 0-1023 are valid for site codes) then click **Save and Close**. You will now see the card format has been added to the system.



This format can be used for your other cardholders.

Editing Card Formats

The Card Format Editor allows you to modify the card formats that are already in use, whereas the program does not allow you to delete them.

- 1 Select the card format and double click on the record. The **Card Format Definition** window opens. If you make any change to the site code of a card format that is in use, the database is updated accordingly.
- 2 Make the necessary changes and click **Save and Close**. The Offline Lock Interface program displays a message saying "Database Changes Made. Lock needs to be re-programmed."
- 3 You need to generate the program files using **Uplink** and upload to the lock. For more information about generating program files, refer to "Offline Lock Interface" chapter.

Defining a new Magstripe Format



- 1 Run this card through the reader slot, and you will see the screen above.
- 2 Click the Add button or click on the **Add New Card Format** button (+ sign on the toolbar) to bring up the **Card Format Definition** window.
- 3 For this example, we assume that the format details are known to be:
 - Site Code comprises the first four (4) digits
 - Encoded ID comprises the next nine (9) digits
 - Issue Code comprises the last two digits (2) and the = sign is a field separator, a typical meaning for that number
- 4 Total number of digits in this case is 16 (which is less than maximum allowed value of 37 for Magstripe cards)

Note: The system will not allow users to set up two Magstripe card formats that have the same length.

- 5 To create this format, leave the edit box for Site Code Start Position unchanged, then set the Site Code Length to 4 (you can either click to select the text entry box and enter the number 4-even 04 works if you want to save the delete or backspace keystroke) or click the upward pointing arrow at the right hand end of the box four times.
- 6 For a Magstripe card you can use a maximum of six (6) digits for Site Code. Check the **Apply Site Code** check box to instruct the system to include the site code in the format.
- 7 Now set the **Encoded ID Start Position** to five (5), since this field begins immediately after the Site Code field ends. Set the Encoded ID Length to nine (9). The maximum digits that can be used as Encoded ID for a Magstripe card is nine (9).
- 8 Finally, set the **Issue Start Position** to 15, because the separator character (= sign) is not in any of these fields. Set the Issue Code Length to two (2) and the Total Number of Digits to sixteen (16). The maximum digits that can be used as issue code is two (2) for a Magstripe card.
- 9 Check the **Apply Issue Code** check box to instruct the system to verify the issue code and include the issue code in the format.

10 Your window should look like this:

The window is titled "MagStripe Card Format Definition". It has a menu bar with "File" and "Help". The main area contains several input fields and checkboxes:

- ID: 0
- Total Number of Digits: 0
- Caption: (empty)
- Description: (empty)
- Encoded Start Position: 1
- Encoded Length: 0
- Site Code Start Position: 1
- Site Code Length: 0
- Issue Start Position: 1
- Issue Length: 0
- Apply Site Code: ☒
- Apply Issue Code: ☒
- Raw Data (Digits: 16): 1324123456789=01
- Card Format: A table with three columns: Encoded ID, Site Code, Issue Code. The first row shows empty fields.
- Buttons: Show Sample, Clear Data
- Footer: Save and Close, Save and New, Close

11 Now click the **Show Sample** button and you will see this:

The window is titled "MagStripe Card Format Definition". It has a menu bar with "File" and "Help". The main area contains several input fields and checkboxes:

- ID: 0
- Total Number of Digits: 16
- Caption: New Magstripe Format
- Description: (empty)
- Encoded Start Position: 5
- Encoded Length: 9
- Site Code Start Position: 1
- Site Code Length: 4
- Issue Start Position: 15
- Issue Length: 2
- Apply Site Code: ☒
- Apply Issue Code: ☒
- Raw Data (Digits: 16): 1324123456789=01
- Card Format ID = 0 (Digits: 16): A table with three columns: Site Code, Encoded ID, Issue Code. The first row shows 1324, 123456789, = 01.
- Buttons: Show Sample, Clear Data
- Footer: Save and Close, Save and New, Close

12 If you set your **Issue Start Number** too low, you will see this.

MagStripe Card Format Definition

File Help

ID: 0 Total Number of Digits: 16

Caption: New Magstripe format

Description:

Encoded Start Position: 5 Encoded Length: 9

Site Code Start Position: 1 Site Code Length: 4 ☒ Apply Site Code

Issue Start Position: 14 Issue Length: 2 ☒ Apply Issue Code

Raw Data (Digits: 16): 1324123456789=01

Card Format ID = 0 (Digits: 16)

Site Code	Encoded ID	Issue Code
1324	123456789	=0

Show Sample Clear Data

Save and Close Save and New Close

So it is always a good idea to look at the way the format splits up the various code fields to ensure that your format is captured correctly.

13 Now enter a unique caption for this format in the Caption field and any additional information in the Description field. Click **Save and Close**.

14 You will see this:

Notice that the CardFormatID is chosen for you to be the next available number.

Card Format Editor

File Help

Available MagStripe Formats

CardFormatID	Caption	Description	Digits
7	Schlage SMS Encoded Card	Format 1 in GRINX 08	12
180	Locknetic 16 digits mag card w/7-d site code	Format #66 in GRINX Fiwe_09.hex	16
2001	New Magstripe format		16

Raw Data (Digits: 16): 1324123456789=01

Card Format ID = 2001 (Digits: 16)

Site Code	Encoded ID	Issue Code
1324	123456789	= 01

Show Sample Clear Data

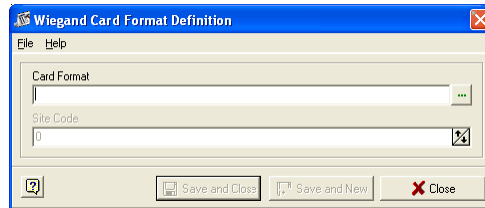
Add Edit Delete

MagStripe Card Formats Used in this System

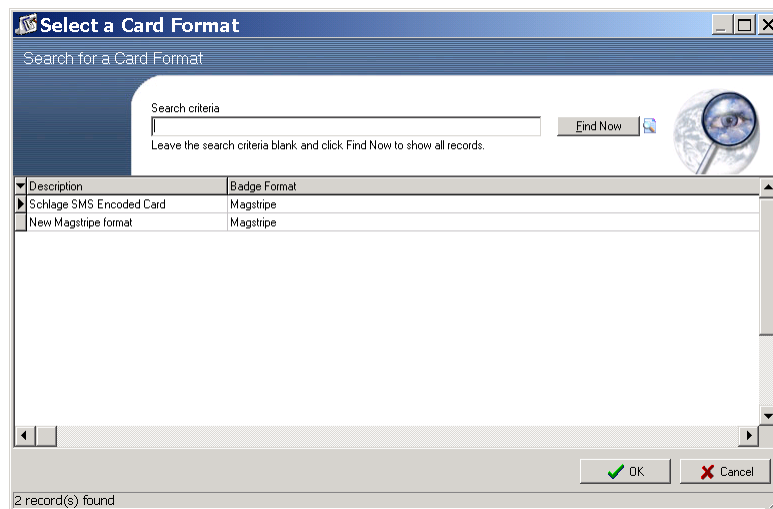
Select a new format to be used in this system

Adding a Card Format in the System

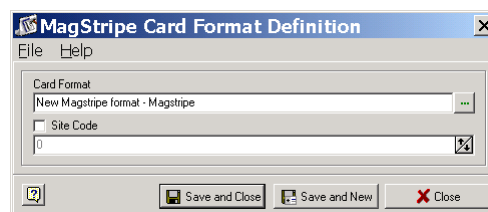
- 1 Click the + (Select a new card format to be used in the system) toolbar button as shown above to add the card format in the system. You will see:



- 2 Click on the browse (three dots) button to the right of the Card Format. You will see:



- 3 Click on the bottom line, which you have just added, then on the OK button and you will see:



- 4 Since you are using Site Code, check the Site Code box and then enter the actual numbers which will be constant across all cards using this format. Use the arrows to increase and decrease the values or enter the numbers directly. Values between 0-1023 are valid for site codes.
- 5 Now click on **Save and Close** to add this card format in the system and return to the Card Format Editor main screen. (Note that the new format is now in the list of Magstripe Card Formats Used in this System.)
- 6 Click Save and New to save the record and add another format in the system. If you click **Close**, instead of Save and Close, the window will close without adding the card format in the system.

Defining a Wiegand Format

- 1 Click on the insert button (+) or click the **Add** button. This will open the **Wiegand Card Format Definition** window.

- 2 Steps for adding a Wiegand format are similar to adding a Magstripe format. The differences are:
- 3 The raw data is represented as bits and only binary numbers can be added in the Wiegand Raw Data field.
- 4 The maximum value for the total number of bits is forty eight (48).
- 5 The maximum value for the encoded ID for a Wiegand card is thirty two (32).
- 6 For a Wiegand card you can use a maximum of nineteen (19) bits for site code.
- 7 Click on the **Available Wiegand Card Format** tab.

Add Card Formats in the System

Once you have created your card format, the next step is adding it to the system.

- 1 In the **Card Format Editor** application, see the **Wiegand Card Formats Used in this System** section. Click the plus button (+) to add your card format.
- 2 The **Wiegand Card Format Definition** window open.
- 3 Select the card format by clicking on the browse button near the **Card Format** field.
- 4 Now enter the site code. You can use the arrows to increase and decrease the value.
- 5 Click **Save and Close** to add the card format in the system and return to the **Card Format Editor** window. Click **Save and New** to save the record and add another format in the system. Click **Close** the close the application without adding the card format in the system.

System Security

CHAPTER 7

Introduction

The **Schlage SMS** offers ample flexibility for the administrator to establish and customize different security groups and assign appropriate levels of privileges to each group. These privileges determine what all programs and functionality an operator can see or use when he/she opens the system. This program helps to significantly improve protection across all the data stored in the system.

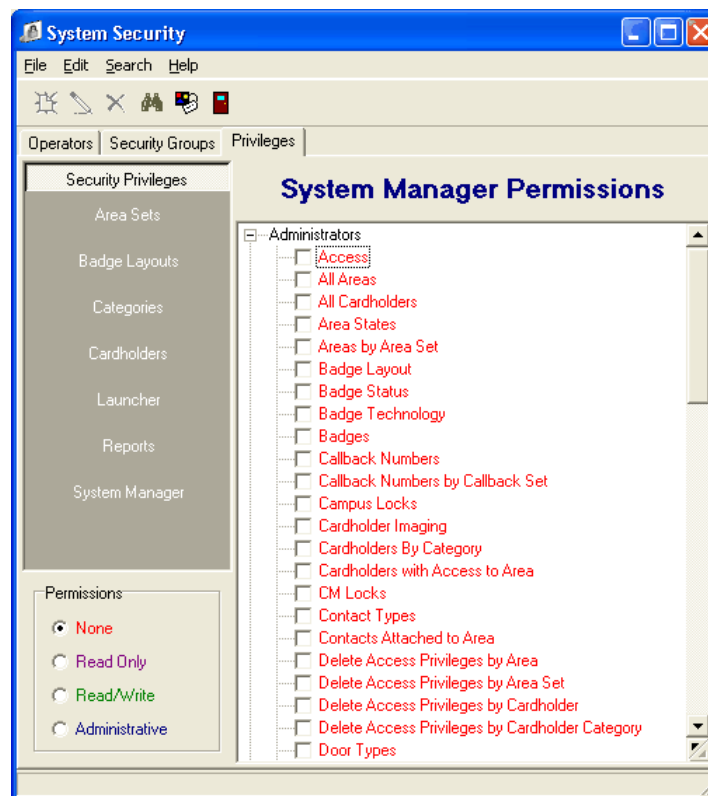
Accessing the application

- 1 Double click on the **System Launcher** icon located on your desktop or choose **Start>Programs>Schlage>Schlage SMS**.
- 2 Login to the system using your assigned user id and password. Double click on the **System Security** icon in the launcher window. This will open the system security main window.

Schlage SMS Select System Security

Users can now add security groups, and assign privileges in **Schlage SMS Select** software. Operators can enable or disable various security privileges. Privileges can be assigned for Area Sets, Badge Layouts, Cardholder Categories, Cardholder Permissions, System Launcher items, Reports, and System Manager fields. Instructions for defining these settings are covered in this chapter.

The screen capture below shows the security settings available for Schlage SMS Select software.



Working with System Security

Overview

As an operator is entered in the module, he/she must be assigned to an individual security group. The database permissions are allocated to each group under the **Privileges** (see "Assigning security privileges" on page 204) tab. The programs that launch before login such as Alarm Monitor, System Processor and CIM are added through the Startup tab.

The Launcher tab defines the applications that will be made available in the System Launcher module and in turn under the System Launcher Permissions of the Privileges tab. Additional rights are assigned to security groups under the Launcher option of the Privileges tab. Non-Schlage programs can also be added to the launcher. When you first open the **System Security** program, by default the program will open the Operator's folder. System Administrator is a factory set operator. There are five main folders in the System Security.

- **Operators**
- **Security Groups**
- **Launcher**
- **Startup**
- **Privileges**

We will discuss each folder in detail in this chapter.

Note: Operators, Security Groups, and Privileges tabs are available in **Schlage SMS Select** software.

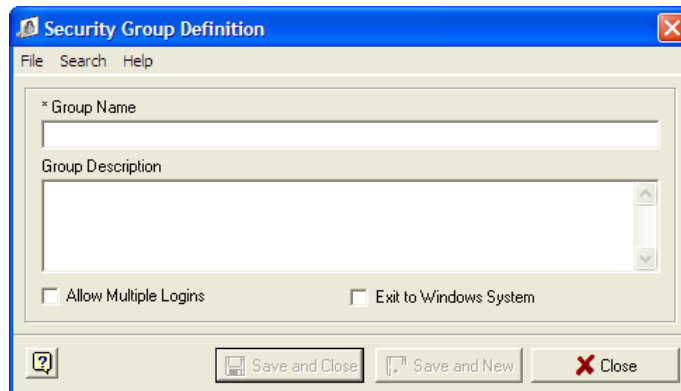
Adding Security Groups


The **Security Groups** folder is where you create several groups depending on your company's needs and later assign privileges to each group. All the operators must be assigned to any of these groups based on what are the different security permissions you want them to have.

The different fields of Security Group folder displays information related to each group. You can create as many groups as you like. It is the privileges (Privileges are discussed in detail in the later parts of this chapter) that distinguish each group from the other. For example you may create 3 different security groups with 3 different levels of privileges. First, you can create Security Group Level 1 and assign all the high level privileges to the system. Then define a group with mid level privileges and later define a third group with low level privileges.

Follow these steps to define a security group.

- 1 To add a security group in the system, click on the **Add** icon on the tool bar. (You can also add from the **Edit** command in the menu bar or by doing a right click on your mouse and select **Add** from the menu.

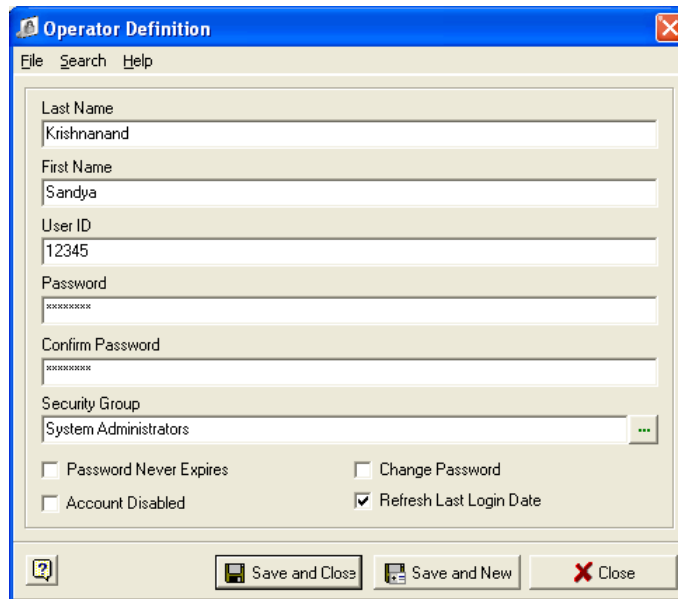


- 2 Once you click the **Add** button the **Security Group Maintenance** window is displayed. Here you have to insert information about the security group you are going to create.
- 3 The following are the different fields and options you will see on this window.
 - a) **Group Name** - Give a name to the security group.
 - b) **Group Description** - Enter the specific information that will identify the group. For example you can enter the type of permission this particular group have.
 - c) **Allow Multiple Logins** - Checking this option allows the operator to log into multiple workstations at a time. If this option is not selected, the operators under this security group will only be able to log on to one workstation at one time.
 - d) **Exit to Windows Systems** - If this option is selected the operator will be able to exit from the **Schlage SMS**. He/she will be able to close all applications. Otherwise the **Exit** button will be disabled and the user will be only able to log out from the system.
 - e) The system also allows you to create duplicate security groups along with the same security privileges of an existing security group. Click the  **Duplicate Security Group** icon and the **Security Group Definition** window opens. Add a group name, description, and then save the definition. The security privileges assigned to the original security group are copied to the duplicate group. If modifications are made to the original group, and duplicate icon is clicked before saving changes, the user is prompted to save the changes.

- f) Click **Save and Close** to save the information and exit the window, click **Save and New** if you want to save the current information and create a new security group. Click **Close** to exit the window without saving.

Add an Operator

- 1 The Operator tab is where you define new operators/users to the system. All the operators defined in the system will be displayed on this window regardless of which security group they are assigned to.



- 2 Select the operator button and click **Add** from the **Edit** menu.
- 3 Fill in the following fields with appropriate information:
- a) **Last Name** - With your mouse point click in the first field and enter your last name. (Once your cursor is blinking in the first field, you can use your tab key on your keyboard to move to the next field.)
 - b) **First Name** - Enter your first name here.
 - c) **User ID** - The user id can be anything you choose, but it must be unique and cannot be duplicated. Also, the user id always defaults to capital letters regardless of how you type it in.
 - d) **Enter Password** - Next, enter a password. The password is case sensitive. However you enter password here that is how it must be entered by the operator to gain access to the system.
 - e) **Confirm Password** - Re-enter the password you entered above to confirm it.
 - f) **Security Group** - By default there will be one factory set security group. That is Schlage System Administrator. This particular security group has all the security privileges to the system. The operator will have same privileges that are set to the group that the operator is assigned to.

Note: Defining Security Groups and assigning Privileges to these groups will be discussed later in this chapter.

- 4 The right side of the operator entry form has four items listed. You can enable these options by placing a checkmark in the box next to each item.

- a) **Password never expires** - Placing a checkmark here will make this operator's password valid indefinitely. If this is not checked, the password will expire on the date it is defined in the Login Requirements. Checking this option will override the number of days a password is valid in the Login Requirements.
 - b) **Change password** - Placing a checkmark here will force the operator to change his or her password after the initial log in. This will protect the operator since the existing password is assigned by the administrator.
 - c) **Account Disabled** - If you want to disable an account place a checkmark here. That particular operator will not be able to log into the system without re-enabling the account.
- 5 There can be situations that you may need to disable an operator to force him/her to come to you before logging into the system. You can perform this function by going to the Operator's folder and double clicking on the operator's name. The **Operator Entry** window will pop up and you can disable or enable the account.
- a) **Refresh Last Login Date** - Checking this option makes the system always refresh the last log in date.
- 6 Click **OK** when you have completed adding operators. If you want to add a new operator click on the **New Operator** button.

Viewing Attachments

Attachments option allows you to see which operators are added to each Security Group.

- 1 Highlight any one group from the **Security Group** folder. You must have at least one operator attached to the group you are viewing.
- 2 Click on the **View** menu on the tool bar. You can see that the **Attachments** option is now enabled (this feature works only with Security Group folder). Click on Attachments. All the operators attached to the selected security group are displayed in a different window. The retired operators are indicated by displaying the related fields in red.
- 3 This feature helps the administrator to verify which operators are attached to each group and make changes if necessary.



Operators attached to Security Officer Level 1 are displayed here. Retired operators are shown in the red fields.

Modifying and deleting operators

Operators are modified within the Operator Entry window.

- 1 Click the **Modify** icon or choose Edit-Modify from the menu bar or right click or double click in the Operator grid to enable the screen.

Note: If the Operator is already connected, the user id and password editing is disabled.

- 2 The **Operator Entry** window is displayed. Edit the information and click **OK**.

Note: The operator has to log out and log back into the system for any security permission modifications to take effect.

- 3 To delete an **Operator**, right click on the Operator Name and select the option *Delete*. You can also choose the Delete option from the tool bar or from the **Edit** menu.

- 4 An active Operator who is deleted is placed in the *Retired Operator* status. Their information remains in the database and is stored under the Retired Operator window. **Active** and **Retired Operators** screens are chosen under the View menu bar.

Note: Deleting a retired operator will remove their information from the database. To retrieve this data, a database restore would need to be performed using a prior backup.

Define Login Requirements

All the operators are forced to conform to the login requirements defined in the system.

- 1 Click on the **File** menu and select **Login Requirements** or select **Edit Login Requirements** button from the tool bar. Fill in the fields appropriately. Each option is analyzed in the following section.

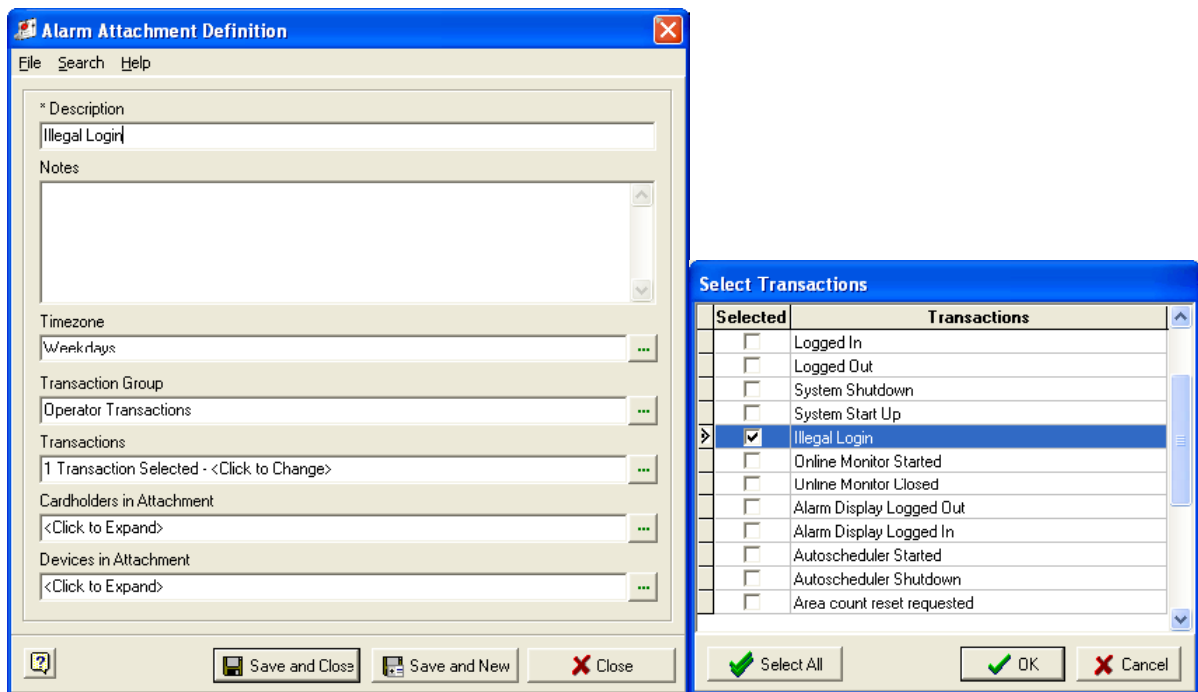
Login Requirements

Minimum Number of Characters in Password:	Number of days of non-usage before disabled:
5	90
Number of days a password is valid:	Number of days to inhibit duplicate passwords:
90	9999999
Consecutive illegal login attempts allowed:	Days in advance to warn of expiration:
3	7
<input type="checkbox"/> With Illegal Login Attempt	
<input checked="" type="checkbox"/> Lockout Workstation for Minutes 15	<input type="checkbox"/> Require Upper/Lower Case Mix
<input type="checkbox"/> Disable the Offending Account	<input type="checkbox"/> Require Alpha/Numeric Mix
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Login Requirement Definitions

- 1 **Minimum number of characters in password** - Enter the minimum number that the password must contain. This feature is used to customize passwords.

- 2 **Number of days a password is valid** - Insert the number of days a password will be valid for. The maximum number you can enter is 999.
- 3 **Consecutive illegal login attempts allowed** - Enter how many times an operator is allowed to attempt to log on.
- 4 **Lockout workstation for minutes** - By placing a checkmark here, the system gets locked out after the operator reaches the maximum number of login attempts allowed. The maximum value you can enter in this field is 999.
- 5 Follow these steps to create alarm whenever an illegal login occurs.
 - a) Open the **Alarm Definitions** program. Define an alarm label called *Illegal Login*.
 - b) Click the + sign on the alarm attachment section to open the **Alarm Attachment** window. Select *Operator Transactions* as Transaction Group, and *Illegal Login* as Transaction.



- 6 **Disable the offending account** - An account will become disabled once the illegal login attempts reach the specified number. Default is unchecked. Once the account becomes disabled the administrator has to uncheck this option for giving the operator access to the system.
- 7 **Number of days of non-usage before disabled** - An operator account is disabled when an operator has not logged on for a specified number of days. Default is 90 days; maximum is 999.
- 8 **Number of days to inhibit duplicate passwords** - This option inhibits users from re-using your previously used password for a specified period of time. This is an added security to the system. The default value is 0. The maximum value allowed is 999.
- 9 **Days in advance to warn of expiration** - Defines when an operator should be warned that the password is about to expire. Default is 7 days.

Note: Password Never Expires option in the **Operator Entry** window will override this field.

- 10 **Require upper/lower case mix** - Lets you define the requirements for a password.

- 11 **Require alpha/numeric mix** - Lets you define the requirements for a password entry.

Define Launcher Items

All the applications you want to open through Schlage Launcher must be added to the launcher folder in the System Security. (This folder also works in conjunction with the Privileges folder.) You must have at least *Read Only* rights to each applications, for them appear on the launcher screen. All the **Schlage SMS** applications (including add on) will be already added to the launcher by default when you purchase the system. You can also add any Windows applications that are on the PC to the System Launcher.

A brief note on permissions

Schlage applications

Schlage applications can have None, Read-Only and Read-Write privileges. To view the applications a user must have a minimum of read only rights. If a user has *none* rights to an application he/she will not see that application in the system launcher and will not have access to it. If a user has *Read only* rights the user will be able to see the application in the launcher but will not be able to write to it.

If a user has *Read-Write* privilege, he/she will have access to the applications and will be able to write to it. Permissions are assigned to Security Groups and users (operators) are assigned to these groups later.

When you install the system, security groups will have Administrator (Read/Write) rights to all the modules that are included in the system. You can modify the rights later on, and if you upgrade the system, the system retains the existing privileges. The security groups will have Administrative rights to any new module that is added during the upgrade process.

Windows applications

Non **Schlage SMS** modules are confined to none-rights or read-write only but not to read only.

Adding applications to the System Launcher

- 1 To add an application to the launcher select the **Launcher** folder and click on the **Add** option from the **Edit** menu.
- 2 You can also add an application by right clicking on the mouse and selecting Add from the menu. Once you click Add option, the system will direct you to the Schlage Bin folder (on the local drive for your machine). Browse through and select the applications you want to add. Click Open.
- 3 The two windows that open are **Select A System Application** (on top) and **Launcher Items**. By default the **Bin** directory will be the **Look In** tab. If the application to be added does not reside in the Bin directory, browse the folders and click on the application you want to add and click **Open**. The Launcher Items window will become active with your selection appearing in the Application to Execute field (*.exe).
- 4 Enter the Caption (i.e. System Security) and a description then click **OK** to exit or **New Application** to add another application. To open the **Select A System Application** window from the Launcher Items window, click the expand button in the **Application to execute** field.
- 5 Select the option **Uses Access Control Security**. By default this field is set to true because Schlage applications won't start unless that check box is checked. When this field is true, the program is launched with Schlage permissions (i.e. permissions assigned to the Security Group that the Operator is a member of). When a third party program is added to the System Launcher such as MS Word or Excel (etc.), we advise that this box be unchecked. Schlage has no control over the privileges assigned to third party applications.

Modifying Launcher Items

- 1 To modify Launcher items choose the **Modify** icon, **Edit>Modify** from the menu bar, right click or double click in the Launcher grid to enable the screen.
- 2 To delete an item, highlight it and click the **Delete** icon, choose **Edit>Delete** from the menu bar or right click in the Launcher grid.

Note: Never delete the **SecurityV5.exe** application from the System Administrator's account. All Users will be prevented from accessing the database and the **Schlage SMS** software must be reloaded.

Adding applications to the Start up tab

The Startup tab, allows you to add certain applications so that the application(s) will start automatically when System Launcher is executed.

- 1 It is recommended that the **System Processor (SP)**, the **Communications Interface Module (CIM)**, **Alarm Monitor**, **Alarm Graphics*** and the **History Archive** be put into the startup tab only for the workstations you want them to run on.
- 2 **Alarm Monitor** or **Alarm Graphics** must be in Startup for each workstation that is defined as an Alarm workstation. In order to add alarm Monitor in the Start up, you need to have at least one alarm defined in the system. The system does not allow adding both Alarm Graphics and Alarm Monitor as start up items. The system launches only either one of these applications automatically. If you try to add both the applications in the Start Up tab, you get an error message. The Alarm Graphics application has a built in Alarm Monitor.
- 3 **The System Processor** should be in Startup on Servers and stand alone machines. There is only one SP per system.
- 4 **CIM** should be in Startup for any machine that has a CIM defined for it.
- 5 **History Archive** should be in Startup and run on the server or on any workstation that will always be running, as it is a scheduled task and will not run if the **Schlage SMS** is not running on the workstation. Remember, most users will probably never see the server. Refer to the chapter on History Archive for details.
- 6 Follow these directions to add an application to the Start up tab.
- 7 To add an application to Startup, click the **Add** icon and the **Select Application to Start Automatically** window opens.
- 8 Highlight the icon of an available application and click **OK**. The application appears in the **Startup** window and is removed from the **Select Application** screen. Only files that are necessary for the system to function are available in the **Select Application To Start Automatically** Window.
- 9 To remove an application from **Startup** simply highlight the icon and choose one of the delete options. This function will remove the application from launching prior to login and will return it to the **Select Applications To Start Automatically** screen.

Assigning security privileges

An administrator can grant different levels of privileges to operator groups by assigning *Read -only*, *Read/Write*, *Administrative* and *None* permissions. This is accomplished through the **Privileges** tab in the System Security module. The three sections of the Privileges tab are the **Security Privileges Bar**, the **Security Group Tree** and the **Permissions** Section.

The fields that display in the Security Tree are dependent on the selection made on the Privileges bar. Security Permissions are assigned to individual Security Groups by expanding the tree below the group's name. Assigned rights are color-coded.

By default, all permissions are set to *none* until the administrator reassigns a privilege therefore rights display in green until permissions are changed.

Note: New records added to the database are automatically given none permissions.

Remember that this includes every type of record, whether it's a new module, report, user defined cardholder field, etc. We recommend that the Security Permissions are reviewed and updated accordingly as records are added.



- 1 To assign privileges, select an option from the **Security Privileges Bar** (top left) and then expand the **Security Group Tree** to view all of its related fields.
- 2 Put a checkmark in the box to the left of the field(s), then click in the color-coded **Permissions** section (this works well for selecting multiple items to be assigned the same permissions).

Clicking on an item also selects the field (this will appear as a broken- line border around the field), but only one item at a time can be chosen and you will not see a check mark appear in the box.

Note: It is recommended that selections be made by placing checkmarks in the boxes as opposed to highlighting the text in order to prevent erroneous assignments, as well as for the ability to make multiple selections.

- 3 The assigned fields will display in the permission's color (None, Read Only, Read/Write and Administrative).
- 4 To provide tighter levels of access control, additional privileges for Area Sets, Categories and Cardholders are available on the Security Privileges Bar.

Note: The Administrative permissions and the Read/Write permissions are functionally the same in current versions of the **Schlage SMS** software. Both settings will give the operator Read/Write privileges.

- 5 Customizing rights is achieved by assigning rights in the System Manager Permission screen and then combining them with additional permissions within related sections.
- 6 The following section is a list of **Security Privileges Bar Options** including some descriptions and examples of how Permissions are assigned to Groups.

Filter Permissions

- 1 Select **Filters** and make your selection(s) from the Online filter Permissions Screen.
- 2 Click on the type of permissions that you want the group to have for them in the **Permissions** section.
- 3 If you set the permissions as *None*, the group will not see the Filter.
- 4 Setting the Filter permission as *Read Only*, allows the group to see and use the Filter, but modifications are not permitted.
- 5 *Read/Write* permissions allow the group to view, edit and delete filters.

Area Set Permissions

The following section describes the effects *None*, *Read Only*, *Read/Write* or *Administrative* permissions have on the area sets.

None permissions

- 1 Select a security group and assign *None* permissions to all the **Area Sets** defined in the system. This will prevent the user from seeing all the Area records defined in the system. The insert button in the **All Areas** tab will be hidden and the operator cannot add new Areas in the system.

Note: The operator can add new area sets in the system if he/she has at least **Read Only** permission to **Area by Area Set** tab in the **System Manager**. The operator has **Read/Write** permissions to the new area sets.

- 2 When all the Area Set permissions are set to None, the cardholders with Area Access do not display in the grid window.
- 3 To define a new Area in the system, the operator should have *Read Only* or *Read/Write* permissions to at least one Area Set.
- 4 To prevent a group of operators from viewing one particular area set, select the area set you want to hide and set the permission as **None**. You need to also make sure that **All Areas** Area Set is also set to **None**.

Read only permissions

- 1 Select a security group. From the **Area Set Permissions** screen, select an area and set permissions as **Read Only**. Make sure that **All Areas** Area Set is set as **None**. The operator will be able to see only the areas under the Area Set you set as **Read Only**. The operators under this security group will not be able to delete or modify this Area Set while allowing them to add (insert button is active) new areas to this area set.

- 2 Select a security group and set all the **Area Set** permissions to **None** while leaving **All Areas** Area Set as **Read Only** or **Read Write**. The operators under this security group will not be forced to select an Area Set while adding new Areas. The new Areas defined in the system will be automatically added to the **All Areas** Area Set. When **All Areas** Area Set is **None**, the user is forced to select an Area Set while defining a new Area.
- 3 It is also important to note that, you should have at least *Read Only* permissions to Areas and Area Sets tab in the System Manager to add new Areas.

Note: If you have at least **Read Only** permissions to **All Areas** Area Set, you will be able to see all the areas defined in the system.

Read/Write or administrative permissions

- 1 **Select an Area Set and assign** *Read/Write* permissions to a security group. The operators under this group will be able to view, edit and delete this area set.
- 2 *Read/Write* permissions to the All Areas Area Set allow the operator to view, edit and delete the entire Area definitions. The operator will be able to define new Areas and will not be forced to select an Area Set for the Area.

Note: If an Area defined in the system is assigned to two different Area Sets and these Area Sets have different permissions (E.g. None, Read Only), the operator will have the maximum permissions to that Area. The **System Manager** Permissions for **All Areas** and **Areas By Area Set** override Area Sets privileges. For example, when Area Set permissions are Read/Write but System Manager Permissions for All Areas and Areas By Area Set are set for None, members of the group will have no rights to Areas, Area Set, Area By Area Set and/or Area Access.

System Manager Permissions

System Manager Permissions are assigned the same way for this option as in all others.

All the tabs and options available in the System Manager module can be controlled by setting different types of permissions.

- 1 In **System Manager** permissions, setting the permission as *None* to the fields available on this screen makes these options hidden or not available in the System Manager module.
- 2 The following section describes the results of setting different System Manager field permissions as **None**, **Read Only** and **Read Write** respectively.

None Permissions

- a) Access - The Area Access tab is hidden. The operator cannot extend or deny area access privileges to a cardholder.
- b) All Cardholders - The All Cardholders tab in the System Manager is not visible. The View All Cardholders option is not available.
- c) Area States - In the System Manager View menu, Area States option is not available. While assigning access control privileges the option area state will not be available.
- d) Areas by Area Set - In System Manager the Areas by Area Set tab is invisible. The users cannot see the entire Areas database.
- e) Badge Layout - Badge Layout option is not available while adding badges. Although badge layout is invisible on badge definition form, a layout can be added by using the Print Badge, Select Badge Layout and Preview Badge layout options on File menu and toolbar icons.
- f) Credential Status - In System Manager Credential Status option is hidden in the Edit menu.

- g) Credential Technology - From the System Manager Edit menu, Badge Technologies option is invisible. The Badge Technology definition window is invisible.
- h) Credentials - In Cardholder Definition program the File menu for active and retired credentials will be grayed out and will not be accessible. Also the Credential Criteria tab in the Advance fine will be invisible. You cannot run the search.
- i) Callback Numbers - The callback numbers defined in the system are hidden from the operator.
- j) Callback Sets - All the callback sets defined in the system are hidden.
- k) Cardholder Imaging - This feature will be hidden to an operator.
- l) Campus Locks - Campus locks tab is hidden to the operator.
- m) Cardholders by Category - This tab will be hidden. The operator can not define new cardholder categories. The operator can still view cardholder records if he/she has at least *Read Only* permissions to categories.
- n) Cardholder with Access to Area - This functionality is invisible in the System Manager and the operator does not have access to these records.
- o) Contact Types - Contacts defined in the system are invisible to the security group.
- p) Contacts Attached to an Area - The operator cannot see this functionality in the System Manager.
- q) CM Locks - CM Locks tab is hidden to the operator.
- r) Delete Access Privileges by Area - The button Delete All Area Access Privileges is invisible.
- s) Delete Access Privileges by Area Set - The operator do not have permissions to delete records. The button for Delete All Area privileges for Cardholders in the Selected Area Set is hidden.
- t) Delete Access Privileges by Cardholder - The button Delete Access Privileges of Selected Cardholders is hidden to the operator in the security group.
- u) Delete Access Privileges by Cardholder Category - This functionality is hidden from the operator. The operator cannot delete the access control privileges of cardholders by category.
- v) Door types - The door types defined in the system are not available to the operator in the security group
- w) Edit CIM Ports - This functionality is not available. Edit CIM Ports tab will be hidden. The users can modify or delete the CIM PORTS defined in the system.
- x) Edit Contacts - The contacts defined in the system are hidden to the operator
- y) Edit Controllers- The controllers defined in the system are hidden to the operator.
- z) Edit Relays-The relays defined in the system are hidden to the operator.
- aa) Edit Readers-The readers defined in the system are hidden to the operator.
- bb) Edit Workstations-The workstations defined in the system are hidden to the operator.
- cc) Event Triggers-The triggers defined in the system are hidden to the operator.
- dd) Events-The events defined in the system are hidden to the operator.
- ee) Hardware Map - The tab Hardware Map is hidden in the tree window.
- ff) Holidays - This functionality is hidden. The operator cannot define new holidays or delete the existing ones.
- gg) Holidays by Holiday Sets - This functionality is hidden.
- hh) Magnetic Stripe Template - If the permissions are set to None, this item will not be available for use.
- ii) CM Locks - The operator cannot see the offline locks.
- jj) Reader Templates-The operator cannot see the reader templates.

- kk) Reader Types- The reader types defined in the system are hidden.
- ll) Readers Providing Access To Area - The operator cannot see the readers providing access to an Area.
- mm) Relay Types- The different relay types defined in the system are hidden.
- nn) Relays Attached to an Area - The relays attached to an area is hidden to the operator.
- oo) Report Groups - The report groups are hidden to the operator.
- pp) Report Launcher - This program is hidden to the operator.
- qq) Site Codes - This functionality is hidden to the operator.
- rr) Site Codes by Site code Sets - This functionality is hidden to the operator.
- ss) Time Zones - The time zones defined in the system are hidden to the operator.
- tt) User Definable Fields - User definable fields defined in the system are hidden to the operator.

Read Only

Setting the permission to *Read Only* allows the user to view the definitions for these fields. For example, if the group has *Read Only* permissions to the fields like call back numbers, time zones, holiday sets etc., the group will be able to view the field and assign these fields while giving access control rights to cardholders, but will not be able to make modifications.

- a) Access - The Area Access tab in System Manager is visible. The users can select an area and view the cardholders with area access and readers providing access to that area. The users can also view the relays and contacts attached to that area. However, the operator cannot modify the area access privileges of a cardholder with *Read Only* permissions to access tab.

Note: To view a certain area or area set, the user should also have at least Read Only privilege to that area or area set.

- b) All Cardholders - The All Cardholders tab in the System Manager is visible. The users can not add or delete or modify cardholder records. The View All Cardholders option is available.
- c) Area States - In the System Manager Edit menu, Area States option is available. The users can not edit or delete an area state. Caption and description of Area State are protected fields.
- d) Areas by Area Set - In System Manager the Areas by Area Set tab is visible. The users can not make any modifications.
- e) Badge Layout - Badge Layout option is available while adding a badge. The users cannot modify or delete a badge layout. The users can add new layouts using Badge Creation program.
- f) Credential Status - In System Manager Credential Status option is available in the Edit menu. While giving access control privileges the Badge Status option is available. The users can not make any modifications to these definitions.
- g) Credential Technology - From the System Manager Edit menu, Badge Technologies option is available. The users can not make any details or modifications to these definitions.
- h) Credential - The users can view all the defined badges for cardholders. The users also should have at least Read Only rights to at least one cardholder category to view the cardholder in that category. The badge criteria tab is visible and the users can run the search query.
- i) Callback Numbers - The operator can see the callback numbers defined in the system. However, the add, edit, delete icons are inactive.
- j) Callback Numbers by Callback Sets - The user can see callback sets defined in the system. Modifications are not allowed.
- k) Cardholder Imaging - The operator can view a cardholder image and its dimensions. Modifications are not permitted.

- l) Cardholders by Category - The cardholder category tab is visible. The operator can define new cardholder categories in the system. The operator cannot edit cardholder records. To see cardholder records, the operator must have at least *Read Only* rights to categories.
- m) Cardholder with Access to Area - The operator can view the records, but does not have permissions to modify or delete any records. The operator can not extend cardholder's area access permissions.
- n) Campus Locks - The campus locks that are already defined in the system are available for the operator for assigning access. Add, delete, edit options are not available.
- o) CM Locks - The CM Locks that are already defined in the system are available for the operator for assigning access. Add, delete, edit options are not available.
- p) Contact Types - The operator can see all the contact types, but do not have permissions to modify or delete the records. The operator cannot add new records also.
- q) Contacts Attached to an Area - The operator can see the records, but do not have permissions to modify or delete the records.
- r) Delete Access Privileges by Area - the operator cannot delete the access privileges to an area. A message is displayed.
- s) Delete Access Privileges by Area Set - The operator do not have permissions to delete records.
- t) Delete Access Privileges by Cardholder -The operator cannot delete the access privileges of cardholders.
- u) Delete Access Privileges by Cardholder Category - The operator do not have the privilege to delete the area access permissions of cardholders in the categories.
- v) Door Types - The operator can see the door types defined in the system and cannot modify or delete them.
- w) Edit CIM Ports - The operator's can see the tab about cannot add, modify or delete the CIM PORTS defined in the system.
- x) Edit Contacts - The operator can view the contacts defined in the system.
- y) Edit Controllers- The operator can view the controllers defined in the system.
- z) Edit Relays-The operator can view the relays defined in the system.
- aa) Edit Readers-The operator can view the readers defined in the system.
- bb) Edit Workstations-The operator can view the workstations defined in the system.
- cc) Event Triggers-The operator can view the event triggers defined in the system.
- dd) Events-The operator can view the events defined in the system.
- ee) Hardware Map - The tab Hardware Map is active in the tree window.
- ff) Holidays - The operator can view holidays defined in the system.
- gg) Holidays by Holiday Sets - The operator can view holiday sets defined in the system.
- hh) Magnetic Stripe Templates - When this field is set to Read Only, the operator can see the menu item, but cannot add, delete, or modify Magstripe templates.
- ii) Reader Templates-The operator can view readers defined as templates in the system.
- jj) Offline Locks - The operator can view the offline locks.
- kk) Reader Types-The operator can view reader types defined in the system. The operator cannot delete the factory set reader types.
- ll) Readers Providing Access To Area - The operator can view the readers attached to an Area or Area Set.

- mm) Relay Types-The operator can view relay types defined in the system. The operator cannot delete the factory set relay types.
- nn) Relays Attached to an Area - The operator can view the relays attached to an Area.
- oo) Report Groups -The operator can view the Report Groups defined in the system.
- pp) Report Launcher - The operator can access reports in Report Launcher program.
- qq) Site Codes - The operator can view delete site codes defined in the system.
- rr) Site Codes by Site code Sets - The operator can view site code sets and site codes defined in the system.
- ss) Time Zones -The user can view time zones defined in the system.
- tt) User Definable Fields - The user can view user definable fields defined in the system.

Read/Write or administrative permissions

- a) Access - The Area Access tab in System Manager is visible. Add, edit, delete icons are active. The operator can extend or delete area access privileges of a cardholder. To select a certain area or area set, the user should also have at least *Read Only* privilege to that area or area set.
- b) All Cardholders - The **All Cardholders** tab in the System Manager is active. The users can define new cardholders in the system. Also the delete and edit icons are active. The **View All Cardholders** option is available.
- c) Area States - In the System Manager View menu, Area States option is available. The user can view, edit and delete an area state.
- d) Areas by Area Set - In System Manager the Areas by Area Set tab is visible. View, Edit and delete options are available.
- e) Badge Layout - Badge Layout option is available in the Badge Definition form. The users can view, edit, add and delete a badge layout.
- f) Credential Status - In system Manager Credential Status option is available in the Edit menu. While giving access control privileges the Badge Status option is available. The users can view, add, edit or delete all the Badge Status definitions.
- g) Credential Technology - The users can view, add, edit and delete the badge technology definitions.
- h) Credentials - The users can view, edit and delete all the defined credentials cardholders. The credential criteria tab is visible and the users can run the search query. The users also should have at least *Read Only* rights to at least one cardholder category to view the cardholders in that category.
- i) Callback Numbers - The users can define new call back numbers and make modification to the existing one.
- j) Callback Numbers by Callback Sets - The user can View, add, edit and delete callback sets.
- k) Cardholder Imaging - The operator can view, add, edit and delete cardholder portraits.
- l) Cardholders by Category - The cardholder category tab is visible. The operator can add, edit or delete cardholder records. To see cardholder records, the operator must have at least *Read Only* rights to categories and Cardholder Definition program.
- m) Cardholders with Access to Area - The operator can view, edit and delete records. The operator can assign area access to cardholders. The operator has the privilege to extend a cardholder's area access permissions.
- n) Campus Locks - The operator can view, add, edit, and delete campus locks in the system.
- o) CM Locks - The operator can view, add, edit, and delete campus locks in the system.
- p) Contact Types - The operator can add, edit or delete the contact types. The operator cannot delete a factory set contact type.

- q) Contacts Attached to an Area - The operator has the privilege to add, edit or delete the records. The operator can attach new contacts to Areas.
- r) Delete Access Privileges by Area - The operator can delete the access privileges of an area. If the privileges are deleted, the area will not provide access to any cardholders.
- s) Delete Access Privileges by Area Set - The operator can delete the access privileges of Area Sets. Select an Area Set and click on the button Delete All Area privileges for Cardholders in the Selected Area Set. A confirmation message is displayed saying that the Areas in this Area Set will no longer provide access to any cardholders.
- t) Delete Access Privileges by Cardholder - The operator can delete the access privileges of cardholders. Select a cardholder from the All Cardholders tab and click on the button Delete the Access Privileges for Selected Cardholder. A confirmation message is displayed saying that this cardholder will no longer have access to any areas defined in the system.
- u) Delete Access Privileges by Cardholder Category - Click on the button Delete Access Privileges of all the cardholders in the Selected Category button. A confirmation message is displayed to say that the cardholders in this category will not have access to any area defined in the system. The operator can delete the access control privileges of all the cardholders in a category.
- v) Door Types - The operator can view, add, edit and delete the door types defined in the system.
- w) Edit CIM Ports - The operator's can view, add, modify or delete the CIM PORTS defined in the system.
- x) Edit Contacts - The operator can view, add, edit and delete the contacts defined in the system.
- y) Edit Controllers- The operator can view, add, edit and delete the controllers defined in the system.
- z) Edit Relays-The operator can view, add, edit and delete the relays defined in the system.
- aa) Edit Readers-The operator can view, add, edit and delete the readers defined in the system.
- bb) Edit Workstations-The operator can view, add, edit and delete the workstations defined in the system.
- cc) Event Triggers-The operator can view, add, edit and delete the event triggers defined in the system.
- dd) Events-The operator can view, add, edit and delete the events defined in the system.
- ee) Hardware Map - The tab Hardware Map is active in the tree window.
- ff) Holidays - The operator can view, add, edit and delete holidays in the system.
- gg) Holidays by Holiday Sets - The operator can view, add, edit and delete holiday sets in the system.
- hh) Magnetic Stripe Templates - When this field is set to Read/Write, the operator can add, delete or modify Magstripe templates.
- ii) Offline Locks - The operator can view, modify or delete the offline lock records.
- jj) Reader Templates-The operator can add, edit and delete readers as templates.
- kk) Reader Types-The operator can view, add, edit and delete reader types in the system. The operator cannot delete the factory set reader types.
- ll) Readers Providing Access To Area - The operator can view the readers attached to an Area or Area Set.
- mm) Relay Types - The operator can view, add, edit and delete the relay types in the system. The operator cannot delete the factory set relay types.
- nn) Relays Attached to an Area - The operator can view the relays attached to an Area.
- oo) Report Groups-The operator can view, add, edit and delete the Report Groups in the system.
- pp) Report Launcher - The operator can view, add, edit and delete reports in Report Launcher program.
- qq) Site Codes - The operator can view, add, edit and delete site codes in the system.

- rr) Site Codes by Site code Sets - The operator can view, add, edit and delete site code sets and site codes in the system.
- ss) Time Zones -The user can view, add, edit and delete time zones in the system.
- tt) User Definable Fields - The user can view, edit and delete user definable fields in the system.

Badge Layout Permissions

Privileges to select, view or print badges will be based on the operator's security group permissions.

- 1 Select a security group and click on the + sign to expand it. You can see all the available badge layouts.
- 2 Choose a badge layout and select none, read-only, read-write or administrative permissions.
 - a) When permission to a layout equals **None**, selecting, viewing or printing that layout will not be available.
 - b) If privilege is set to **Read-only**, the operator can see the badge layout, but operator cannot create, modify, duplicate or delete the badge layout.
 - c) If the operator has **Read/Write** or administrative permissions to a badge layout, he/she can view, create, modify, duplicate or delete the layout.

Cardholder Category Permissions

None permissions

- 1 Setting all cardholder categories in the **Cardholder Category Permissions** screen to *None* prevents a group from viewing the entire cardholder database.
- 2 Under **Cardholder Category Permissions** screen, select a cardholder category and set the privileges as *None*. (**All Cardholders** Category should also be set to *None*) This prevents a group from viewing any cardholders in that category. The cardholder records under this category will not show up in any of the search results as well as find routines. This is an effective way to prevent a group from viewing the entire cardholder database. Permissions can be determined on a need to know basis
- 3 If permissions for **All Cardholders** is set to *None* then they must be a member of some other valid cardholder category to have Area Access. Without valid Category privileges, the cardholder will not appear in the All Cardholders database. An example follows.
- 4 There are multiple buildings spanning several cities or countries and employees who travel between various locations. The System Administrator has created a **Cardholder Category** in the System Manager called Traveling Service Representatives. Additional categories have been created that are unique to each client location.
- 5 Traveling employees have been given access to Areas and Area Sets in their home office building as well as various other buildings that they visit:
- 6 From the Cardholder Category Permissions window:
 - a) Category and Cardholder By Category additions, modifications and deletions for their location are enabled.
 - b) Traveling Service Representatives privileges are set to Read Only
 - c) Members of the Traveling Service Representative category will display in the All Cardholders tab of the System Manager module and access at the reader level will be granted. Users in various locations can view cardholder fields for these cardholders, but cannot change any information.

Note: If in **System Manager Permissions** screen, **Cardholders by Category** field permissions are set to **Read Only** or **Read/Write (Administrative)** the operator can add new cardholder categories in the system. The operator will have Read/Write privileges to the newly defined categories.

Read only permissions

- 1 Select, **All Cardholders** Field from the **Cardholder Category Permissions** screen and set the permission as *Read Only*. All Cardholders field will display on the Cardholder Category window. Every cardholder in the database can be viewed in the All Cardholders tab and pop up window. Cardholder records cannot be edited or deleted.
- 2 Select any Category from the **Cardholder Category Permissions** screen and set permissions as *Read Only* while setting **All Cardholders** field permissions to *None*. This prevents a group from viewing the entire database while allowing them to see a group of cardholders. Group will not have permission to drag and drop a Cardholder in a *Read Only* Cardholder Category.

Read/Write or administrative permissions

- 1 With **Read/Write** permissions to **All Cardholders** tab under **Cardholder Category Permissions** screen, every cardholder in the database can be viewed in and pop up window. This right does not control insert, edit or delete privileges. Full access to the Cardholder database is granted. Additions, modifications and deletions are permitted.
- 2 Select a cardholder category and assign the permissions as Read/Write for a security group while leaving all other category permissions defined in the system as *None*. The operators in this security group will be able to view, edit and delete only those cardholder records in the cardholder category to which he/she has Read/Write permissions.

Note: To edit a cardholder record, the operator must have Read/Write or administrative rights to the cardholder fields that he/she wants to edit.

Cardholder Category

The following are the different types of security privileges that can be assigned to different cardholder categories and the effects they will have on the cardholder records.

None - Any cardholder record within a cardholder category with a permissions flag of *None* will not be visible to the user and therefore, cannot be edited by the user. The cardholder record will not show up in any search dialog or find routine during the session. None permissions on a cardholder record based on the category overrides any permission defined under Cardholder Column Security.

Read Only - Any cardholder record within a cardholder category with a permissions flag of 'read only' will be visible to the operator. However, the record and all fields of that record cannot be edited by the operator. This permission setting overrides any read/write permissions defined under Cardholder Column Security.

Read/Write or Administrative – Any cardholder record within a cardholder category with a permissions flag of 'read/write' will be visible to the operator and can be edited by that operator. However, even though the operator might have read/write to the cardholder record, the Cardholder Column security settings override the read/write on an individual column level.

Cardholder Field Permissions

The administrator can secure the individual cardholder information fields such as Last Name, First Name, Initial, and User Defined Fields etc. in the Cardholder Definition program by assigning different levels of privileges to each field. These fields are also shown within the **All Cardholders** tab of System Manager. These fields are listed separately under **Cardholder Field Permissions** in System Security. The System Administrator can control which fields can be viewed, inserted, modified and deleted.

This gives the System Administrator the versatility to assign a combination of permissions within the main screen and its sub screens.

- 1 The group cannot see any of the cardholder fields if all the field permissions are set as *None*.
- 2 The group can only view these cardholder fields if the permissions are set as *Read/Only*. Edits and Deletion are not permitted.
- 3 To allow a group to insert new cardholders and modify specific fields while hiding certain confidential employee information:
 - a) From System Manager Permissions, select **All Cardholders** and change to *Read/Write*. This Permits user to access the All Cardholder's tab.
 - b) From Cardholder Category Permissions, select either **All Cardholders** or an individual Category and change to *Read/Write*. Permits user to add a new Cardholder to a Cardholder Category.
 - c) From Cardholder Field Permissions, select the fields the group has to modify and change to *Read/Write*.
 - d) Select the fields that shall be hidden from the group and assign permissions as *None*.

The system allows users to modify a single cardholder field though the user does not have Read/Write privileges to the required fields in the module. For example, the user can have Read/Write privilege to the Notes field, but still cannot edit any other cardholder fields.

Override Sets and Reports

Manual Overrides and Report Sets that have been defined in the system appear in under these options.

- 1 Check the boxes next to report groups, and assign permissions by selecting the appropriate permissions from the left hand pane. Now expand the group, and assign permissions to each report.
- 2 If the permissions are set to None, the override sets and reports selected will be hidden from the user.
- 3 *Read Only* permission allows the user to view and execute an override set, but modifications are not permitted. *Read Only* permissions to reports allow the user to view a selected report.
- 4 *Read/Write* permissions allow the user to view, edit and delete override sets and Reports. However the user cannot delete factory set reports.

Note: You need to assign privileges to individual reports under the reports group in order for the privileges to take effect. Expand the reports group header, select the report and then assign the privileges.

Badge Creation

CHAPTER 8

Introduction

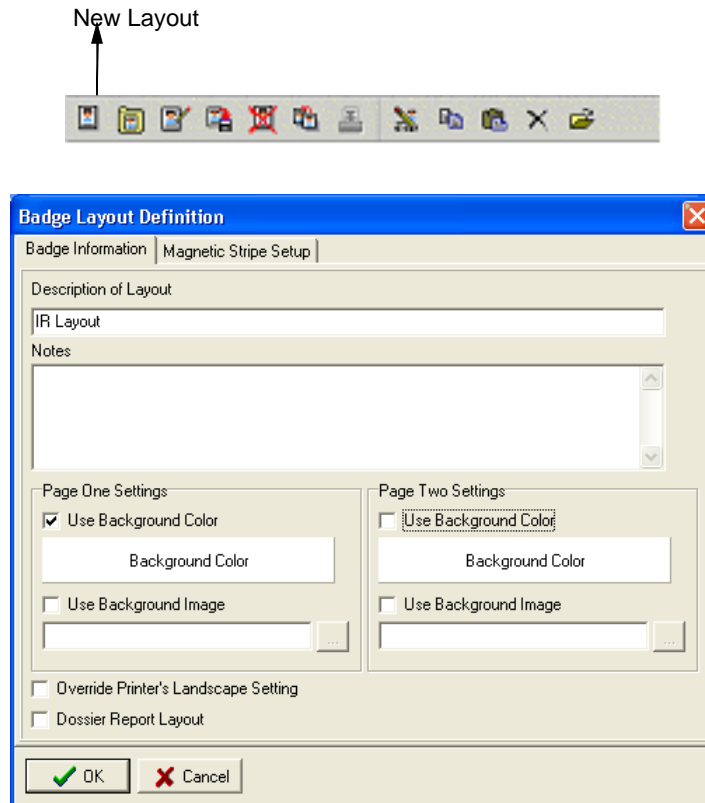
The **Badge Creation** software is designed to be the easiest tool for creating and maintaining identification badges. It comes with the standard list of features including background colors and images, annotation controls and double sided printing. The annotation controls provide users with the ability to insert fields such as logos, pictures, signatures, text, cardholder fields or a variation of fields using the Expression Builder Wizard. Using these controls provide you with the versatility to choose from a selection of borders, bar code settings, font styles, image settings such as transparency, ghosting and colors as well as four rotation selections. All these great features packed with a powerful and flexible design interface offers you the opportunity to design a professional badge layout (*JPG, BMP, and GIF are the supports image formats*).

Accessing the application

- 1 Open the Launcher by double clicking the **Schlage SMS** icon on your desktop or go to Start>Programs>Schlage SMS> Schlage SMS.
- 2 In the login window, enter your user ID and password.
- 3 In the **System Launcher** window, double click on **Badge Creation** icon.

Defining a new badge layout

- 1 Select **File>New Layout** or click on the New Layout icon from the tool bar to display the **Badge Layout Definition** form. This window is subdivided into two tabs; the **Badge Information** tab and the **Magnetic Stripe Setup** tab. The program defaults to the **Badge Information** tab.



- 2 Enter a description for your new layout in the **Description of Layout** field. This field allows a maximum of 64 characters.
- 3 Enter the notes in the **Notes** field. This field allows 255 characters.
- 4 If you want to use a background color for your layout, checkmark the option Use Background Color and select a color by clicking on the color field below. You can select colors using the Color Palette. If you want to select a custom color click on Define Custom Colors on the Color window.
- 5 If you are using a background image for your badge, checkmark the option Use Background Image. Click on the expand button to select your image file. The Background Image field defaults to the Schlage\Data\Graphics folder. Select an image in the file folder and the image is centered on the badge by default. When both the features (background color and background image) are used, the image becomes transparent to allow the color to show through.

Note: The Background Image field is used for company logos or a picture that are displayed on all badges that will use the layout. Individual employee pictures (cardholder images) are inserted using Annotation Controls.

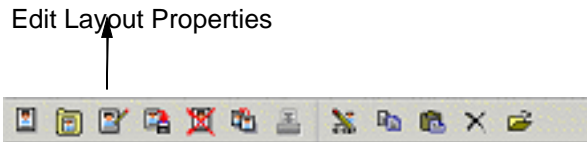
- 6 If you are creating a double-sided badge you need to select background color and image for page one and two.

- 7 Select the **Override Printers Landscape Settings** option to ignore the default Printer Settings for Landscape. The Badge Creation module examines the dimensions of the badge and determines the proper settings for the layout.
- 8 When the Dossier Report Layout option is checked, the **Badge Layout** is marked as a Dossier.
- 9 The cardholder badges that use a dossier layout can be sent to any printer and produce a hard copy on standard sized paper. Dossier Reports are printed from the Cardholder Definition module. These reports are printed when it is necessary to have paper copies of badges.
- 10 If you are going to have a magnetic stripe card, select the **Magnetic Stripe Setup** tab to define three tracks for magnetic swipe cards. Placing a check mark in the **Enable Magnetic Stripe Encoding** activates the track boxes. These tracks are defined using the Expression Field Wizard. Click the expand button to the right of a track field to launch the **Expression Field Wizard**. In the **Expression Builder**, click on the **Insert Field** Button to enter your information.
- 11 In the Expression Field Wizard select the file type. You can select hard coded text, cardholder field or field separator. click Next.
 - a) Hard coded text is manually entered and appears exactly as you type it. When using this choice it should be tailored to fit all cardholders that will be assigned the badge layout.
 - b) Cardholder Field accesses your database tables to provide a selection of all cardholder fields and User Defined fields.
 - c) Field Separator places the ^ symbol within the track expression. This separates the track fields from one another.
- 12 If you have selected the option hardcoded text, type in your information in the empty field. If you have selected Cardholder field, click on the expand button next to the empty field and all the cardholder fields defined in your system are displayed. Select the field you want to use and click **OK**. If you want to separate the track fields, you can insert a field separator.
- 13 Expression formulas operate by replacing the field name with actual cardholder data. For instance, if you choose First Name, it will draw the person's first name from the database and insert it in the stripe. If **Employee Number** is chosen, the cardholder's unique employee number will be encoded in the magnetic stripe.
- 14 The size of the data field can be specified by selecting Fixed Width Sizing or Variable Sizing.
 - a) **Fixed Width Sizing** - Enter a value in the empty field using the up and down arrows. The width of the field will be fixed and the user will not be permitted to enter data that is bigger than the size specified here.
 - b) **Variable Sizing** - If this option is selected the field width will adjust according to the size of the data entered.
- 15 You can move the fields up and down by clicking on the **Move Field Up** and **Move Field Down** buttons. Click on the **Remove Field** button to delete a field.
- 16 Once you have defined the **Field Type** and **Field Data** click **Finish** and **OK** to return to the **Badge Layout Definition** window.
- 17 Click **OK** on the definition screen to display your new badge layout.

Note: With your new layout displayed, choose File on the menu bar. All File menu options are activated.

Editing a Badge Layout

- 1 Select **Edit Properties of the Badge Layout** from the **Edit** menu or click on the **Edit Layout Properties** icon from the toolbar.



- 2 This opens the **Badge Layout Definition** window. Make modifications to properties and click **OK**.

Duplicating a Badge Layout

- 1 Open the badge layout you want to duplicate by selecting **Open Existing Badge Layout** option.
- 2 Select the **Duplicate Layout** option from the **File** menu. This opens the **Badge Layout Definition** window of that particular layout. You can make modifications to the layout if there necessary. Click **OK** and the program creates a new layout immediately.

Editing Magstripe Options

- 1 Select the option **Edit Badge Creation Options** from the **Edit** menu.
- 2 On the **Badge Creations** options window, you can edit suffix, prefix and field separator.

Defining annotations for a new Badge Layout

The **Annotation Control** feature gives you the flexibility to plan and customize the data on a badge. They are very important part of the badge, because annotations form the content of your badge layout.

Follow these steps to add an Annotation Control.

- 1 Select **File>Open Annotation Control**.
- 2 Click on the + sign on the **Annotation for** window. The **Annotation Definition** window is displayed.

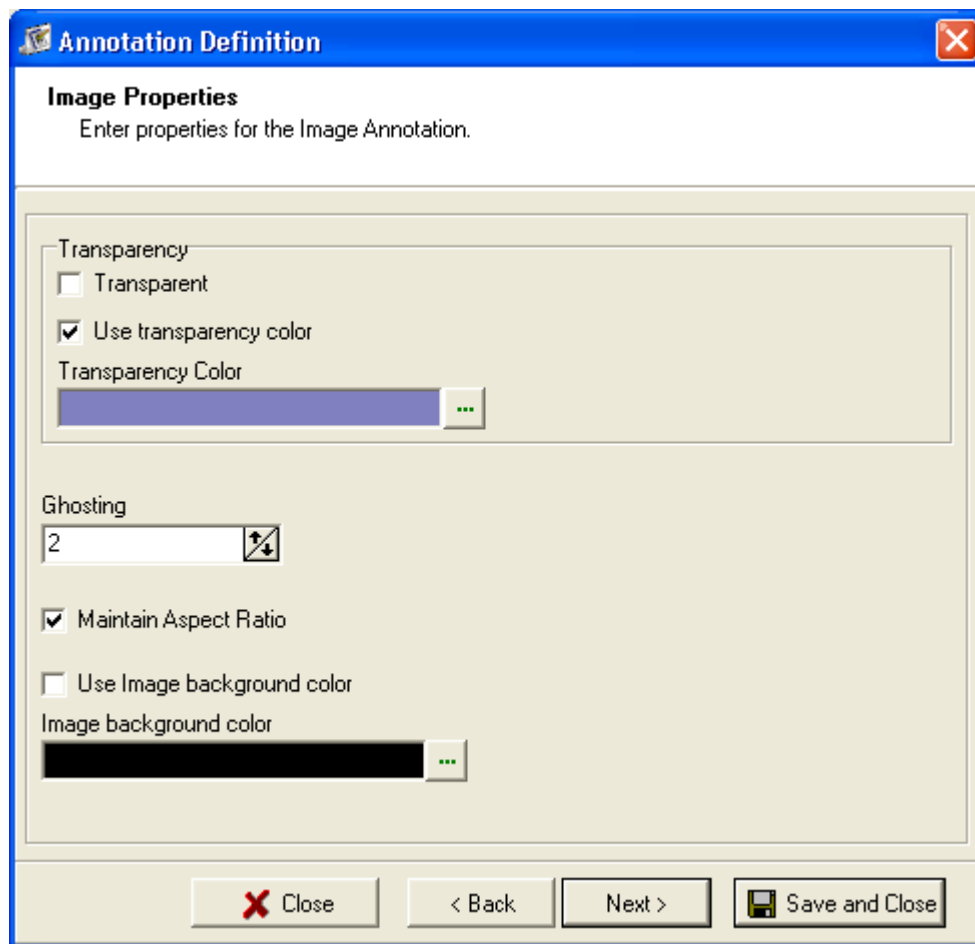
Note: When either a browse button or drop down arrow becomes active, it indicates that more choices are available. It is recommended that you explore each field and become familiar with all selections.

- 3 Enter a description for the new annotation. This field allows 64 characters. For example, if you want to have your company's name on the badge, enter the text "*Company Name*". This is a required field. If you have any comments on this annotation, you can enter that in the **Notes** field. A maximum of 255 characters are allowed in this field. These notes are not displayed on the badge.
- 4 Next select the annotation type. There are nine (9) fields available. They are Cardholder Image, Static Picture, Signature, Cardholder Field, Static text, Expression, Date, Time, and Date and Time. The annotation types are used to streamline the appearance of badges. These annotation types provide the versatility to choose from a selection of borders, bar code settings, font and text styles, image settings such as transparency, ghosting and colors as well as rotation selections.

The annotation types are selected depending on what fields you want the badge to contain. Each annotation type brings up a different set of associated fields with which you can define the annotation. For example, select **Cardholder Image** from the drop down menu. Next, select a sample image. Click on the expand button. The **Select Image** window opens the default Portraits folder. C:\Schlage\Data\Portraits. Select an image from any of the folders can click **Open**.

Note: The bar code enabled option is only available with Cardholder Field, Static Text, Expression, date, time, and date and time fields.

- 5 Click **Next** to continue to modify the properties of the image. If you are satisfied with the annotation click **Save and Close**. If you click **Next** the image properties are displayed.



- 6 If the annotation type is an image, the following are the associated fields available.
 - a) **Transparency** - This option is most often used in conjunction with the Cardholder Image, Static Picture or Signature annotation types. In order for transparency to work, your background must be a consistent shade of one color and have no shadows. The background shade is replaced to appear transparent. Your background should be a color that generally would not appear on a subject.

Note: It is highly recommended that your camera be placed in a fixed position on a tripod and a blue or green background screen be used to reduce the occurrence of shadows.

Refer to the user manual of your specific camera for best results. This is why special effects crews that are making movies use a "Blue Screen" or a "Green Screen" to remove background shadows and colors. If the background cannot be a consistent shade, you should not attempt to use transparency.

- b) **Use Transparency Color** - Click on the expand button to select a color to test the transparency effect.
 - c) **Ghosting** - Removes and grays all pixels in the picture; this is sometimes called opacity. It gives the image a watermark effect. More opacity is applied by increasing the number and therefore the lighter the image.
 - d) **Maintain Aspect Ratio** - Select this option to resize the image to fit within the annotation box and still maintain its original proportions. When this feature is turned off, the image will stretch to fit the entire annotation box. It is recommended that you always select this feature. It is automatically turned on for images.
 - e) **Use Image Background Color** - If this feature is checked, it will use the background color to fill in your annotation background. It also turns transparency on to allow the color to show through. When using this feature, the image should be made with transparency in mind.
 - f) Click the **Next** button to use the other available options. These options are available with all the annotation types.
 - **Border Settings** - Select border width and a border color. This places a colored border around the annotation.
 - **Add Prefix** - Select this option to add a prefix to the annotation. Enter text in the empty field.
 - **Add a Suffix** - Select this option to add a prefix to the annotation. Enter text in the empty field.
 - **Rotation** -This is a pull down option that offers these choices: None, 90, 180 and 270 Degree Rotation.
- 7 Click **Save and Close**. A confirmation message is displayed. Click **Yes** to add the annotation on the badge layout. This places the annotation on the top left corner of the layout. You can place the annotation wherever you want by drag and drop method.

Description of Annotation Types

- 1 **Cardholder Image** -This places a default image on the badge layout. The cardholder image that is assigned to the individual will replace this default when the badge is printed.
- 2 **Static Picture** - Opens the Schlage/Data/Graphics folder, once an image is selected it will appear on all layouts. This would usually be the company logo.
- 3 **Signature** -This places a default signature on the layout and is later replaced with the signature that is associated with a cardholder.
- 4 **Cardholder Field** - Allows you to place a Cardholder Field or User Defined field on the badge. It is later replaced with the value associated with that field for a specific cardholder.
- 5 **Static Text** - Whatever is typed in the field will be printed as is on the badge. It is hard-coded text.
- 6 **Expression** - Allows you to build a combination of Cardholder Fields and hard coded text in one annotation. The Expression Builder Wizard will help you to create the formula.

For example, you could place your employee's last name, a comma, a space and their first name on one line of the badge. First choose **Expression** as your Annotation Type. In the "Expression String" field select the ellipse button and select **Insert Field**. Place a check mark in "Cardholder Field" and highlight "Last Name".

- 7 Next select **Hard coded Text** and place a comma in the field. The third step is to insert *Hardcoded Text* again and hit the space bar. Select **Cardholder Field** again and then choose First Name from the list.

- 8 **Date** -This field inserts the actual date on the badge or label at the time of printing.
- 9 **Time** -This field inserts the actual time on the badge or label at the time of printing.
- 10 **Date and Time** -These fields insert both date and time on the badge or label at the time of printing.

Once you have selected the annotation type, there are various associated fields to select from. The following page describes all the fields. However, each annotation type will not display every field.

- 11 **File Name/Field Name/Text** - The value that is entered will depend on the annotation type that was selected.

Bar Code Settings

Bar code settings are available with the Cardholder Field, Static Text, Expression, Date, Time and Date and Time annotation when **Barcode Enabled** option is selected.

Annotation Definition

Barcode Properties
Enter properties for the Barcode Annotation.

Barcode Type Code 39	Barcode Height 1.00
Background Color	Left Margin 0.02
Foreground Color	Top Margin 0.02
Narrow Bar Width 0.02	Wide to Narrow Ratio 2.50

☐ Add Check Digit
 ☐ Add Check Digit To Text
 ☐ Show Text

Code 128 Character Set: AUTO

 Codabar Character Set: Start Char [] Stop Char []

- 1 **Barcode Type** - Select the barcode font.
- 2 **Barcode Height** - Change the height of the bars in the annotation.
- 3 **Background Color** - Set a color for the background of the annotation.
- 4 **Foreground Color** - Set a color for the bars on the annotation.

- 5 **Left Margin** - Set the left margin in centimeters
- 6 **Top Margin** - Set the top margin in centimeters.
- 7 **Narrow Bar Width** - Set the width in centimeters of the narrow bars.
- 8 **Wide to Narrow Ratio** - Set the wide to narrow ratio on barcodes that only contain narrow and wide bars such as Code 39, Interleaved 2 of 5 and MSI.
- 9 **Add Check Digit** - Add the check digit to the barcode. The check digit is required for all the bar codes except Code 39, Industrial 2 of 5 and Code bar.
- 10 **Add Check Digit To Text** - Add the check digit that is encoded in the barcode to the human readable text to be displayed.
- 11 **Show Text** - Add the human readable text to be displayed with the barcode.
- 12 **Code 128. Character Set** - Choose the set of characters to be used in code 128.
- 13 **Codabar Character Set** - If the selected barcode type is "Codabar", the Start Char and Stop Char fields are enabled. The start/stop characters are used as a key to read codabar barcodes in the database. The characters selected from the drop down list are valid. The codabar barcode is listed in the badge layout and it is printed on the credential.

Text Styles

If the annotation is text, the following options are available:

- 1 **Font Name** - Click on the expand button to select the font properties. You can select a font, font style, size, color etc. on the **Font** window.
- 2 **All Capital Letters** - Forces upper case letters for all text. This is recommended for the cardholder names.
- 3 **Horizontal Alignment** - Aligns and centers the text within the same section of the annotation rectangle.
- 4 **Vertical Alignment** - Centers the text in the middle of the annotation.
- 5 **Size to Fit Mode** - Three options are available to determine how the text will fit within the annotation.
- 6 **Use Text background Color** - When this feature is checked, the entire annotation rectangle will be filled with the color that is selected.

Border Setting / Date and Time Format Options

The **Options** window allows you to define the border settings and choose pre-defined or custom formats for the date and time annotation type.

Note: The Date and Time Format selection is available only for Date, Time or Date and Time annotation types.

- 1 **Border Settings** - Here you can define the border width and select a color for the border for the annotation.
 - a) **Border Width** - Enter the width of the border manually in the field or use the up and down arrows to adjust the value.
 - b) **Border Color** - Click on the expand button to open the color palette. Choose a color for the annotation border and click OK.
- 2 **Rotation** - This field allows you to rotate the annotation in a specific angle. Click on the arrow next to the field to choose an appropriate angle.

- 3 **Date/Time Formats** - The fields under this option allow you to choose a format for the date and time annotation type.

Note: The Date/Time Formats field is available only when you choose the Date/Time annotation type.

- a) **Date/Time Format** - Click on the drop down menu to choose a pre defined format for date and time. You can also enter your own custom format in the field.

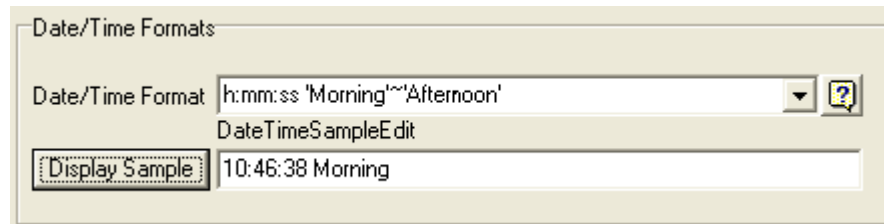
- b) **Display Sample** - Click on this button to view a sample of the format you choose. The system displays the current date and time in the chosen format.

Explanation of different formats used to display date and time:

Format	Details
d	Displays the day as a number without a leading zero (1-31)
dd	Displays the day as a number with a leading zero (01-31)
ddd	Displays the day as an abbreviation (Sun-Sat)
dddd	Displays the day as a full name (Sunday-Saturday)
m	Displays the month as a number without a leading zero (1-12). If the m specifier immediately follows an h or hh specifier, the minute rather than the month is displayed.
mm	Displays the month as a number with a leading zero (01-12). If the mm specifier immediately follows an h or hh specifier, the minute rather than the month is displayed.
mmm	Displays the month in the abbreviated format (Jan-Dec)
mmmm	Displays the name of the month (January-December)
yy	Displays the last two digits of the year (00-99)
yyyy	Displays the year as a four-digit number (0000-9999)
h	Displays the hour without a leading zero (0-23)
hh	Displays the hour with a leading zero (00-23)
n	Displays the minute without a leading zero (0-59)
nn	Displays the minute with a leading zero (00-59)
s	Displays the second without a leading zero (0-59)
ss	Displays the second with a leading zero (00-59)
am/pm	Uses the 12-hour clock for the preceding h or hh specifier, and displays 'am' for any hour before noon, and 'pm' for any hour after noon. The am/pm specifier can use lower, upper, or mixed case, and the result is displayed accordingly.
a/p	Uses the 12-hour clock for the preceding h or hh specifier, and displays 'a' for any hour before noon, and 'p' for any hour after noon. The a/p specifier can use lower, upper, or mixed case, and the result is displayed accordingly.
/	Displays the date separator character.
:	Displays the time separator character.
xx'/"xx	Characters enclosed in single or double quotes are displayed as-is, and do not affect formatting.

Note: In the pre-defined time format, system accepts the time only in the "AM/PM" format (not case sensitive). To use a customized time format, you must use single (') or double quotes (") to enclose the characters, and use the "~" character as a separator for AM/PM.

Example: If you use 'Morning'~'Afternoon', the AM/PM symbol is replaced by 'Morning' or 'Afternoon'.



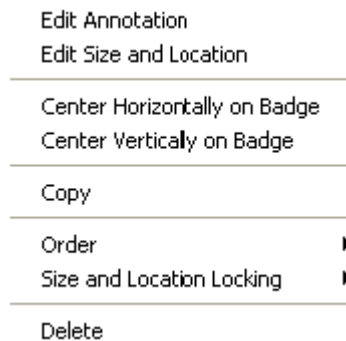
Additional Annotation Design features

You can move an annotation by clicking on it and while holding the mouse button down, drag and drop it to any location within the rectangle. To re-size it, place the mouse on a black dot of the design border until the double-sided arrow appears. While holding the mouse button down, drag and reshape it. To enable the design border choose View from the menu bar and click "Show Design Borders".

To access additional design features, left click on the annotation to highlight it and then right click to view more options.

Editing Annotations

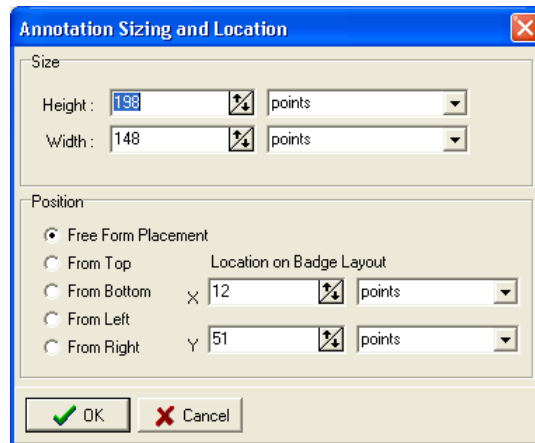
Click on the Annotations menu on the Badge Layout Utility to access the annotation options. These options are also available on the right click menu of the badge layout.



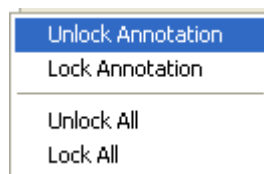
The following options are available from the Annotation menu as well as the right click menu.

- 1 **Edit Annotation** - Opens the Annotation Control window.

- 2 **Edit Size and Location** - Opens the **Annotation Sizing and Location** window allows you to change the dimensions, position and location of the annotation.



- 3 **Center Horizontally on Badge** - Centers on the horizontal plane.
- 4 **Center Vertically on Badge** - Centers annotation in the middle and on the vertical plane of the layout.
- 5 **Copy** - Places annotation on the clipboard for pasting.
- 6 **Order** - Changes the order of the level of the annotation.
- 7 **Size and Location Locking** - These options locks the annotation in place so it cannot be inadvertently changed. Once a badge is approved as the company prototype, it is recommended that you use this feature.



- 8 **Delete** - Deletes the highlighted annotation from the badge layout.

Viewing a double-sided badge

- 1 To view a double-sided badge, select the options **Page One** or **Page Two** from the **View** menu.

Notes on issuing badges to cardholders and printing

- 1 In the **Cardholder Definition** module, use the search feature to select the **Cardholder**. under the tab labeled **Active Badges**, use the **Add Badge** icon to display the Badge Definition screen.

- 2 Verify or add information in the fields of the Cardholder.

- a) **Credential Technology** - Select the type of the credential by clicking on the expand button.
 - b) **Stamped Number** – This is the internal numbering system that your company uses to designate cardholders.
 - c) **Encoded ID** - This number is embedded into the security access card and is unique to each cardholder. An Encoded ID number can be reused **ONLY** if the previous badge has been retired. For both the Stamped Number and Encoded Number, if you have the Enrollment Reader enabled you can simply swipe the badges and the numbers will be entered automatically.
 - d) **Issue Code** - This shows the number of cards issued to this individual, starting with one (1). For example, John Doe lost his first badge with the Issue Code of 1. So you must reissue another badge with the same Stamped Number and Encode Number but the Issue Code will be two (2).
 - e) **Badge Technology** - This is where you can select the type of badge card used.
 - f) **Badge Layout** - Click on the expand button to view all previously designed badges. Each credential created for a cardholder can have only one badge layout attached to it.
- 3 View the badge layout for selected cardholder
 - 4 Print the badge. The system allows you to print multiple copies of the badge at the same time.

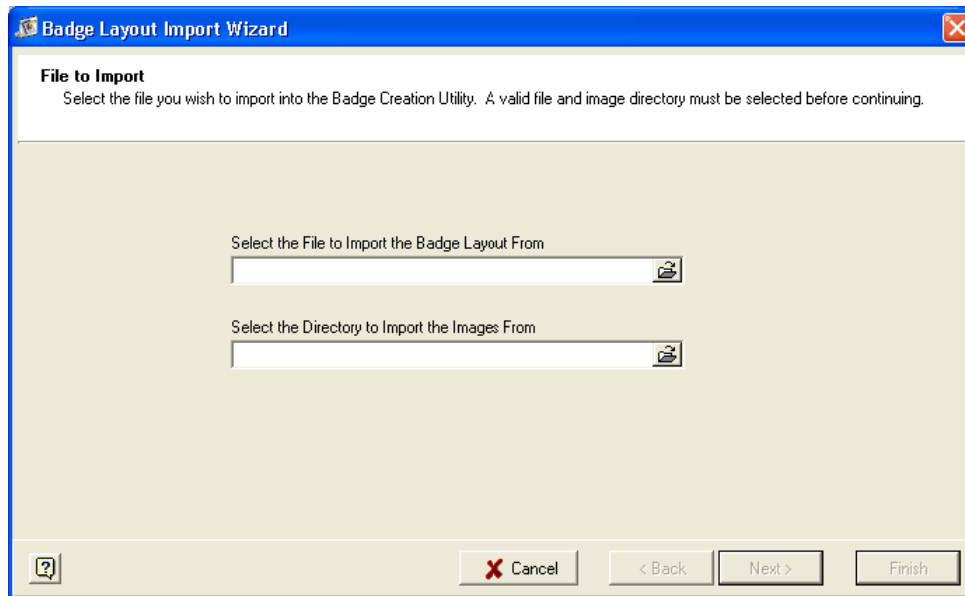
Importing and Exporting Badge Layouts

The **Badge Layout Import-Export** feature allows the user to export and import badge layouts. These options help the user to save the badge layouts as binary files in a specified folder. All the images that are stored in the data/graphic folder are copied to the specified folder. This functionality allows the user to export the binary file and the graphics to wherever they want.

Importing a Badge Layout

Follow these steps to import a badge layout.

- 1 Select **File>Import Badge Layout** option. The **Badge Layout import** wizard is displayed.



- 2 Click the browse button to select the file that will be imported to the layout.

Note: There must be a .bgl file in your file folder to perform this function.

- 3 Next, select existing directory where the badge layout images will be imported.

Note: If the directory you chose here is the factory set graphics folder in the data directory, it is assumed that the graphics are already placed there. The program will copy all the graphic files (bmp, gif, jpg, tif) from the specified import images directory into the data/graphics folder. This is determined by the registry settings created using **RegSetV5.exe**.

- 4 Click **Next**.
- 5 In the next step you have to choose a style for the import. The badge layout can be imported in two ways.
 - a) **Insert a new Badge Layout**
 Inserting a new badge layout creates a completely new badge layout file and does not affect any existing one.
 - b) **Update an Existing Badge Layout**
- 6 Updating an existing badge layout allows you to choose a pre-existing layout, which will be updated with the information from the bgl file. The existing badge layout will be replaced by the newly imported badge layout.
- 7 Click **Next**. A summary of the actions is displayed. If you are satisfied with the process, click **Finish**.
- 8 A message is displayed saying that importing badge layout is complete. The badge layout you imported will be available for badge creation in **Badge Creation Utility**, **Cardholder Definition** program, and **Guest Pass System**.

Exporting Badge Layouts

- 1 Create a folder in the **Schlage SMS** directory or on the network where you want to place your badge layout and image files.
E.g. C:Program Files\Schlage\Data/Layout Exp
C:Program Files\Schlage\Data\Image Exp
- 2 Verify that you have badge layouts with logical naming conventions.
- 3 Select **File>Export Badge Layout** option.
- 4 The **Badge Layout** Export Wizard displays all the available layouts. Select the badge layout you want to export. Click **Next**.
- 5 Next, in the **Badge Layout Export Wizard**, Click the browse button to open **Select Export File** window. Give a file name to save the badge layout you are exporting. Click **Save**.

Note: The directory you choose here must be an existing one. The factory set graphic folder should not be used.

Click the browse button to select a directory to save the images that are exported. After selecting the image directory click **Next** to continue. A summary of the process is displayed.

- 6 If you are satisfied with the process, click **Finish**.
- 7 A message is displayed saying that export badge layout is complete.
- 8 Click **OK** to complete the process.

Note: The bgl file and the graphics files must be copied together to the location where the badge will be imported.

Badge Queue

CHAPTER 9

Introduction

The **Badge Queue** program allows users to store badges and dossier reports prior to printing. Badges and dossiers reports are send to the Queue from the **Cardholder Definition** module or can be added directly from this module. Data in a queue can be printed individually or in batches. Batch printing is useful when multiple badges need to be printed or when badges are not immediately needed and can be printed later.

The operator may define as many queue names that suit the company's needs. A drop down option allows the user to select a specific print queue. Each badge queue allows the selection of a badge printer and a dossier printer. When printing a queue, the program will check the job type of the current item and send it to the correct printer.

Accessing the application

- 1 Open the **System Launcher** by double clicking the launcher icon on your desktop or go to **Start>Programs>Schlage SMS>Schlage SMS**.
- 2 The Login window opens. Enter your user ID and password.
- 3 In the **System Launcher** window, double click on **Badge Queue** icon.

Working with Badge Queue

There are four sections to the main window of Badge Queue program. They are: menu options, tool bar shortcuts, Queues and Badge Queue cardholder grid. You can create as many queues as is necessary for your company. When a badge is selected to print, the operator has a choice to send it to a printer or to select a queue from the Badge Queue list. Highlight a queue name to view all badges assigned to it. The grid on the right, in the Badge Queue section, will display all cardholder badges for that queue that are ready to print.

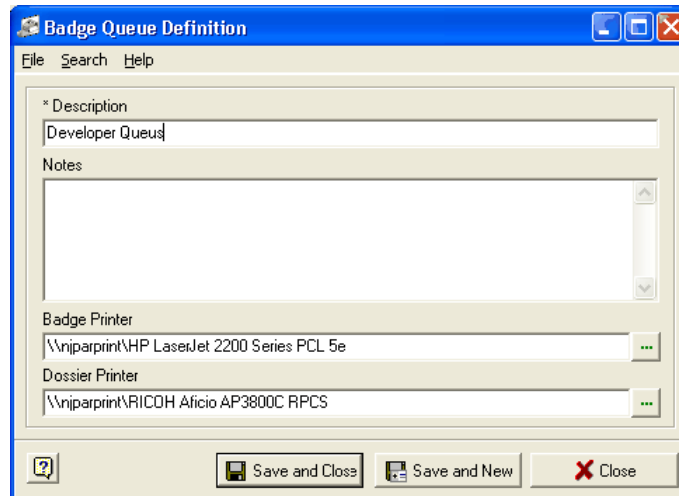
Badge Layouts are viewed by highlighting the cardholder in the Badge Queue grid and choosing View Badge Layout from the View menu or on the tool bar. Highlight a layout in the Badge Queue section and right click for additional options.

Note: Printing of badge layouts will be based on privileges assigned to their security group and according to the Badge Layout security and/or application privileges. The operator can print only those badges to which he/she has permissions to view (Read Only, Read/Write or Admin). When permissions equal None, the operator will be prevented from viewing, selecting or printing layouts.

Badge Queue Definition

Queues are where badges are held until the print queue command is issued.

- 1 To add a Queue directory, use the tool bar shortcut or select **File>New** Badge Queue. The **Badge Queue Definition** window opens.



- 2 Enter the queue description and notes.
- 3 Select a badge printer. Click on the expand button to display all the available printers.
- 4 Now select a dossier printer. Click on the expand button and select a printer from the list.
- 5 Choose **Save and Close** when only one queue is being defined. To add several different queues, select **Save and New**. Selecting **Close** will exit the screen.

File menu options

The following are the menu options available on the **Badge Queue Definition** window.

- 1 The **New** option will open a new definition window.
- 2 **Save** will save the definition and immediately close the screen.
- 3 **Save and New** will save the current definition window then open a new definition screen to add an additional queue.
- 4 **Close** will exit the Badge Queue Definition window.

Once you have defined your Queues, they will display in the main window of the module in the order that they were defined. Highlight the queue name to view cardholders that have been added.

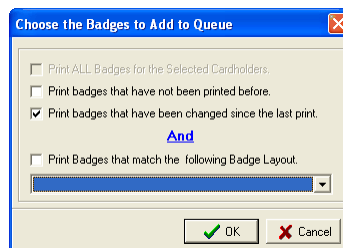
Adding cardholder Badges to the Queue

Cardholders can be added to the queue from the Badge Queue module or from the Cardholder Definition module.

- 1 From the Badge Queue module, highlight a queue, and then select the binocular icon on the tool bar or from the Search menu to activate the Cardholder Search Wizard. Highlight a cardholder record and click **OK**. A print window offers four options.

- a) Print All Badges for the Selected Cardholders:

This is useful when more than one badge per cardholder has been assigned and you need every badge to be printed. When checked, the fourth option "Print badges that match the following Badge Layout" becomes active as well. Use the drop down arrow to select the layout. The second and third choices become disabled.



- b) **Print badges that have not been printed before** - This option searches the cardholder record for the Last Print Date and when empty it will place the layout in the queue. It also activates the third and fourth option but disables the first choice.
 - c) **Print badges that have been changed since the last print** - Select this feature when changes have been made to the badge record and a cardholder's badge needs to be reprinted. The first and second options are available however the fourth is inactive.
 - d) **Print Badges that match the following badge layout** - Allows the operator to select a specific layout. This feature must be used in conjunction with either choice one or two.
 - e) Click **OK**.
- 2 From the Cardholder Definition module:
 - a) Select a record using the Search feature. Under the **Active Badges** tab, highlight a badge and then click on Printer icon on the tool bar. The sub window called **Send to Printer or Queue** opens. Choose **Send Badge To Printer Queue**, click the **Expand** button and select a queue name.
 - b) The cardholder badge will now be held in the printer queue that you have selected until you are ready to print it.

Printing Badges

- 1 To print badge that is in the queue choose **File>Print Badges In Selected Queue** or highlight the queue name and right click. You can also activate the print option by highlighting a queue name and using your right mouse button, select **Print Badges In Selected Queue**. All badges stored in the active queue will begin to print immediately.
- 2 Use the right mouse button in the Cardholder grid list to activate the menu. Select **Print Selected Badge Immediately**. The highlighted badge will be sent to the printer.
- 3 **To erase a badge from the queue**, select **Delete Badge From Queue** from the right click menu in the Cardholder grid list. The highlighted badge is removed from the Badge Queue list.

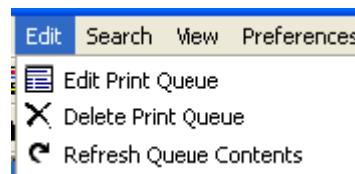
- 4 **Select All** option in the right click menu in the Cardholder grid list will highlight all the badges. When all records are highlighted the print or delete option can be used.
- 5 **Unselect All** reverses the Select All feature.
- 6 **To stop a print job**, select **File>Stop Current Print Job** or select the tool bar icon.
- 7 **Rearranging and resizing the Badge Queue columns**

Change the sort order of a column heading by dragging the column title and dropping it to a new location on the grid.

Columns can also be resized by hanging the cursor over the top right of the column by the line divider. When a two-sided black arrow appears, hold the left mouse button while moving to the right or left.

Editing Queues

The edit menu offers three options.



- 1 **Edit Print Queue** - This opens the **Badge Queue Definition** window. Make your changes and click **Save and Close**.
- 2 **Delete Print Queue** - Click this option to delete the selected badge queue. A confirmation message is displayed.
- 3 **Refresh Queue Contents** - Selecting this option to see all the recent changes that you made.

Viewing a Badge Layout

Highlight a cardholder in the grid list of the active queue then select **Badge Layout** option to view the cardholder's badge.

Search for Badge Queues

The Search feature activates the Badge Queue search wizard. Select the **Find Now** button to list all Badge Queues.

Advanced Find

Using Advanced Find, you can build the search criteria by selecting appropriate entries from the drop down list box and entering specific value in the value field. You have to select a specific field name, condition and a specific search value.

Advance Find feature uses Boolean logic to create complex and highly precise searches. Boolean logic uses three connecting operators (NOT, AND OR) to narrow or broaden a search or exclude a term from the search.

It is the process of linking criteria to narrow or expand a search through the use of **NOT**, **AND** or **OR**.

The Advance Find feature helps the operator to customize the search function. Operator can define the searches and save them for a later use. The saved search criterion is displayed only for the operator who defined it.

- 1 Click on the Advance Find tab located on the top of the **Search** window.
- 2 **The Advanced Find** window opens.
- 3 Define your search criteria.
 - a) If you want to search for **Badge Queue ID = 10**, you need first select the left parenthesis from the list box.
 - b) Parenthesis can be used to create nested search clauses. Using the parenthesis one can override the standard order of priority (left to right) for each Boolean statement in the search.
 - c) Select Badge Queue ID as the Field Name.
 - d) Select equal to = as the condition.
 - e) Enter the value as 10.
- 4 Provide the closing parenthesis at the end.
- 5 If you want to specify additional search condition you can select AND/OR from the list box.

E.g. if you want search Badge Queue IDs between 10 and 20 and between 25 and 30 you could define the search criteria as follows. Use the double parenthesis to nest a search clause.

```
((Badge Queue ID>10) AND (Badge Queue ID <20))  
OR ((Badge Queue ID>25) AND (Badge Queue ID<30))
```

When you run the search you will get records corresponding to Badge Queue ID values between 11 to 19 and 26 to 29.
- 6 When you are satisfied with the criteria, click **Add to List** button. If the criteria is not valid, it is displayed in red under the Where Clause section. When the criteria becomes valid the font color changes to black.
- 7 Once you have defined the criteria click **File>Save**.
- 8 Add a description to your search and click **OK**.
- 9 The new search will be saved and listed under the **Advanced Find** button.

User Defined Fields

CHAPTER 10

Introduction

The **Schlage SMS** provides a tool which allows you to create additional cardholder fields based on your company needs. The user can create these fields in Cardholder Definition module and Guest Pass System. Just a few examples of additional fields are nick name, social security number, telephone extension, home address, home phone number, review or anniversary date. It is a flexible module that allows you to organize and customize the appearance of your cardholder fields in the main display of the Cardholder Definition Module and the Guest Pass System.

The fields defined using the User Defined Field Editor can be displayed in the Transaction Monitor under the Cardholder Transactions Sections. In order to do this you need to select **Include in Transaction Monitor** option while defining new fields.

Note: After creating or editing user defined fields, you must close the **UDF Editor** module to see the changes in the Cardholder Definition or in the Guest Pass System modules.

Accessing the application

- 1 Open the system launcher by double clicking on the launcher icon on your desk top or go to **Start>Programs>Schlage SMS>Schlage SMS**.
- 2 Open the **User Defined Fields Editor** program by double clicking on the icon from the System Launcher.

Working with UDF Editor

The top display window called the **Cardholder Information Display** provides ten cardholder fields. These are the same fields that are listed in the **All Cardholders** tab of **System Manager** and in the information window of the Cardholder Definition module.

They are Last Name, First Name, Initial, Notes, Activation Date, Expiration Date, Controlled anti-pass back, Keypad ID, Cardholder ID and Access Blocked. By default, the information display is viewed in grid format. For easy identification, the **Tab Control Window** located in the bottom section displays these factory set fields in red. They can be organized in any order you like; however, the system will not permit modification or deletion of these fields. Still the system allow to modify the display description of these fields.

- 1 Tab Control tool bar offers five options.
- 2 The **New** button activates the User Defined Field Wizard that is used to define new cardholder fields.

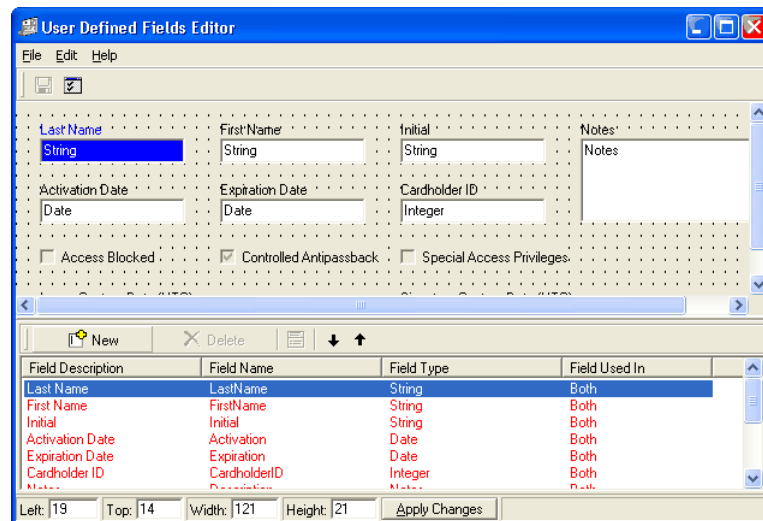
- 3 **Delete** and **Edit** buttons are available only when a User Defined Field is highlighted. These fields are easily identified because they display in green. Factory Set Cardholder fields appear in red. When a hard-coded field is highlighted, the Delete and Edit icons are disabled. **Up** and **Down** arrows control the tab order for the fields in the Cardholder Information window. Once you have rearranged the order of the Cardholder Information fields, it is recommended that the Tab Control fields be sorted in the same order. This is done manually using the Up and Down Arrows.

Note: User can not Add or Delete User Defined Fields while SQL replication is enabled.

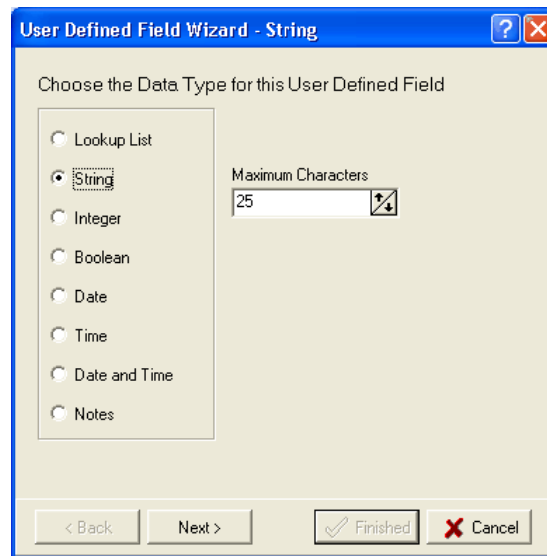
- 4 The data in the **Field Description**, **Field Name** and **Field Type** sections can be placed in any order. To rearrange this list, highlight the field and select one of the arrows on the tool bar. Any field in the UDF Cardholder Information Display can be highlighted, dragged and dropped to a different location in the window. On by default, **Display Grid** shows a network of dots that help you to align the fields. **Snap to Grid** aligns the fields on the page by pulling them to the nearest intersection of grid lines. These settings can be turned off by using **Edit>Options** or the double checked window button on the tool bar. An added convenience to the end user is the ability to set the tab sequence to fields by changing the order of the fields in the Tab Control window. Highlight the field below, then use the Up and Down Arrows on the tool bar. The keyboard tab in Cardholder Definition will follow the order you set here. User-defined fields are displayed in green in the Tab Control section.
- 5 Provided you have the proper security permissions, you may add, delete and modify User Defined fields. As noted above, factory set fields appear in red.

Creating a new User Definable Field

- 1 Click on the **New** button located on the lower pane of the main window.



- 2 In the **UDF Wizard**, select the type of data for the field you are going to define. The eight selections are Look up list, String, Integer, Boolean, Date, Time, Date and Time and Notes. The default field is string with maximum of 25 characters.



Data Type Definitions

The following section gives you a description of each data type available.

Lookup List - This field will create a list menu in the selected module(s) from which the user may choose one item. By expanding the field to open a selection window, the available items will be displayed. Choices added to the menu are called List Items. At least one item must be added in order to create this type of field. For example, you can create a field named Corporate Locations with list selections of New York, London, Paris and Milan.

String - This is a field that allows combinations of characters. It is a commonly selected data type for a User Defined field. Since it permits a combination of numbers and dashes, you can create a field called Social Security Number or use it to create a Nick Name field. String is the default Data Type for the UDF Wizard.

Integer - Is a field that allows the user to select a numeric value. For example, in this screen for Data Type selection, the Maximum Character field is an Integer Data Type.

Boolean - Creates a check box where the value is either true or false. Unchecked equals false (no) while checked equals true (yes). An example is Access Blocked or anti-pass back. If Access Blocked has a check mark in the field then the answer is yes and therefore the cardholder's access will be blocked.

- **Date** - Selecting this data type provides a field with a drop down calendar.
- **Time** - Selecting this data type provides a field with up and down arrows to select the time.
- **Date and Time** - These two fields work the same as the combined Date and Time field.
- **Notes** - A maximum of 255 alphanumeric characters can be entered in this field.

For this example, we will create a User Defined field for "Nick Name." To create the Cardholder Field called "Nick Name" set the maximum characters to 25. This defines the number of characters that will be accepted in the field. In this case, the cardholder's Nick name cannot exceed 25 characters.

Creating a String Field

- 1 Click **Next** on the **Data Type** screen. Next, type in a **Display Description** and the **Field Name**.

The **Display Description** is simply the field name that the user sees in the software. There is a maximum limit of 32 characters.

The **Field Name** is stored within the tables of the database. An end user will not see the database field name. Spaces are not permitted.

- 2 Choose **Next** to open the **Limits and Defaults** window.

Note: The fields present in this window are relative to the field type being created. For example, if you are creating a look up list, you need to define the items in the list.

The following are the options available if you are creating **String** field.

- a) **Component Width** – field display width defaults to 300; it's usually not necessary to change the width.
- b) **Default Value** - This value will be placed in all existing records. It may be modified depending on the information represented by the new field.

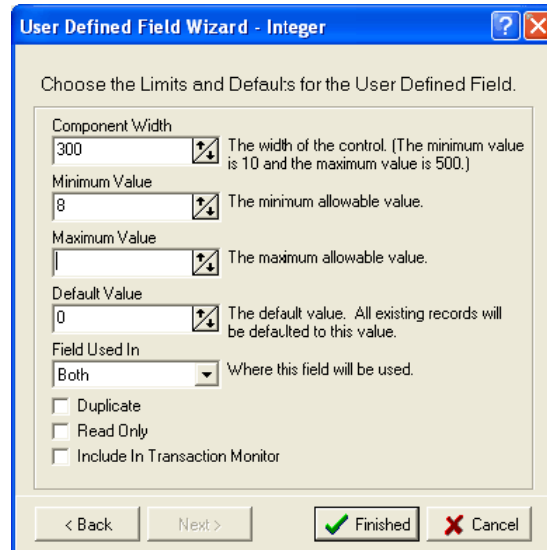
- c) **Field Used In** - You must choose where you wish to use a field.



- 3 In the last window during the process, the Field Used In box will be blank until a selection is made and the selection can be changed later to any of the choices shown above.
- a) To make your UDF a required field, place a select the **Required** check box.
 - b) To allow the UDF to be copied when the **Duplicate Cardholder** feature is used in the **Cardholder Definition** module, select the **Duplicate** check box.
 - c) **Read Only** option will not allow this field to be modified.
 - d) **Include in Transaction Monitor** option will make the field appear on the Cardholder Transactions section of the Transaction Monitor.
 - e) **User Defined Field Template** - Specific requirements can be set here for the type of data to be entered in this field. This helps to maintain data integrity and prevent errors in key fields. Special characters are entered here which allow and/or require alpha, numeric or combined character types. Here are a few commonly used examples:
 - **L** – requires alpha character only (in this position)
 - **I** – permits alpha character only
 - **A** – requires alphanumeric only
 - **a** – permits alphanumeric only
 - **C** – requires arbitrary character
 - **c** – permits arbitrary character
 - **0** – (zero) requires numeric character only
 - **9** – permits numeric character only
- Using a Social Security number as an example, you would enter “000-00-0000” as your template, requiring a numeric character for each position the zero appears in. The dashes are ignored, but appears in the field.
- 4 Click **Finish** to complete the process.

Creating an Integer field

If the data type is an **Integer**, you can see the following additional options in the **Limits and Defaults** window.



The image shows a Windows-style dialog box titled "User Defined Field Wizard - Integer". It contains several input fields and checkboxes. The "Component Width" field is set to 300, with a note: "The width of the control. (The minimum value is 10 and the maximum value is 500.)". The "Minimum Value" field is set to 8, with a note: "The minimum allowable value." The "Maximum Value" field is empty, with a note: "The maximum allowable value." The "Default Value" field is set to 0, with a note: "The default value. All existing records will be defaulted to this value." The "Field Used In" dropdown is set to "Both", with a note: "Where this field will be used." There are three checkboxes: "Duplicate", "Read Only", and "Include In Transaction Monitor", all of which are currently unchecked. At the bottom, there are four buttons: "< Back", "Next >", "Finished" (with a green checkmark icon), and "Cancel" (with a red X icon).

- a) **The width of the control** - This defines size of the field that is created. The default value is 300; it's usually not necessary to change the width.
- b) **The minimum allowable value** - Refers to the minimum number of character allowed in the field.
- c) **The maximum allowable value** - Refers to the maximum number of character allowed in the field
- d) **The default value** - When you open the related program the value you entered here will be present in the field.
- e) To make your UDF a required field, place a select the Required check box.
- f) To allow the UDF to be copied when the **Duplicate Cardholder** feature is used in the **Cardholder Definition** module, select the **Duplicate** check box.
- g) **Read Only** option will not allow this field to be modified.
- h) **Include in Transaction Monitor** option will make the field appear on the Cardholder Transactions section of the Transaction Monitor.

The data types like **Boolean**, **Date**, **Time** and **Notes** use the same options that are described in the above sections.

While creating user defined fields for Date and Time, the value displayed in the field can be set to a user defined default value. Check the option **Use Default Value** and the date and time fields become active. If the **Use Default Value** option is not selected, the current date and time is displayed in the corresponding programs that these fields appears. Enter the value for date in the upper field and the value for time in the lower field. On the date field, click on the down arrow to open the calendar to choose a date. Time can be adjusted using the up and down arrows as well.

The screenshot shows the 'User Defined Field Wizard' dialog box. The title bar reads 'User Defined Field Wizard -'. The main instruction is 'Choose the Limits and Defaults for the User Defined Field.' Below this, there is a section with a checked checkbox labeled 'Use Default Value'. To the right of this checkbox, a message states: 'Use Default Value selected. All existing records will be defaulted to this value.' Below the checkbox, there are two input fields: the top one contains '12/10/2007' and the bottom one contains '12:00:00 PM'. Below these fields is a 'Field Used In' dropdown menu, currently showing a blank space, with the text 'Where this field will be used.' to its right. Further down are four unchecked checkboxes: 'Required', 'Duplicate', 'Read Only', and 'Include In Transaction Monitor'. At the bottom of the dialog are four buttons: '< Back', 'Next >', 'Finished' (with a checkmark icon), and 'Cancel' (with a red X icon).

Creating a Lookup List field

If the data type is a **Look Up list**, select Lookup List as the data type, and add the items to the list.

The screenshot shows the 'User Defined Field Wizard - Lookup List' dialog box. The title bar reads 'User Defined Field Wizard - Lookup List'. The main instruction is 'Add Items to your Lookup List'. On the left, there is a list box containing the following items: NJ, NY, MA, PA, RI. On the right, there is a message: '* Required - It is required that at least one Lookup List Item be added before you can create this User Defined Field. Click the Add the New Item button below to do this.' Below this message are two buttons: 'Add the New Item' and 'Delete the Selected Item'. At the bottom of the dialog are four buttons: '< Back', 'Next >', 'Finished' (with a checkmark icon), and 'Cancel' (with a red X icon).

- a) Here you need to enter the items you want to include in the look up list by clicking **Add the New Item**. Enter the item and click **OK**. The new item is added to the list.

- b) The fields available in the **Limits and Defaults** window is different from all other options.

User Defined Field Wizard - Lookup List

Choose the Limits and Defaults for the User Defined Field.

Component Width: 300. The width of the control. (The minimum value is 10 and the maximum value is 500.)

Default Value: [Empty field with dropdown arrow]. The default value. All existing records will be defaulted to this value.

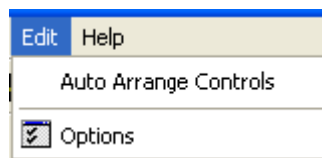
Field Used In: Cardholder Only. Where this field will be used.

☒ Required
☐ Duplicate
☐ Read Only
☐ Include In Transaction Monitor

< Back Next > Finished Cancel

Note: The description for each field on this window is provided in the "Creating a String field" section.

Edit Options



- 1 **Auto Arrange Controls** - This will arrange the fields in the Cardholder Information display according to the size of your window, for the most efficient placement and viewing.
- 2 **Options** - This opens the User Defined Field Settings window. Here you can change the preferences of how you want to view the Cardholder Information display. This is also a tool bar icon.
 - a) **Display Grid** - Select this option to have a network of dotted lines that form a grid to help you align the fields and format the spacing of the fields.
 - b) **Snap to Grid** - The Snap to Grid feature automatically aligns the fields by pulling it into alignment with the nearest intersection of grid lines. A field cannot be placed in between the grid lines.

E-mail Address Editor

CHAPTER 11

Introduction

The **E-mail Address Editor** is a tool that allows the user to store e-mail addresses in the system. The tool has a user friendly interface to capture e-mail addresses and to associate them with the cardholder names. The mass insert option provides the ability to add multiple e-mail addresses at the same time. This tool also can be used to store the e-mail addresses of the recipients of reports. This utility is also equipped with a search feature that allows you to find records easily. The standard tool bar icons provide add, delete, edit, refresh and bookmark icons. The different arrows on the tool bar help you to move between the records easily.

Accessing the application

- 1 Open the **Schlage SMS** software by double clicking on the Schlage SMS icon on your desktop or go to Start>Programs>Schlage SMS>Schlage SMS.
- 2 Enter your assigned user ID and password.
- 3 In the **System Launcher** window, double click on **E-Mail Editor** icon.

Adding e-mail addresses

You can add e-mail addresses in the system in two ways. The first method is to define the e-mail addresses one by one using the e-mail address definition window. This method also provides you an option to associate the address with a cardholder record. Follow these steps to add e-mail addresses individually.

- 1 Click on the + icon to open the **E-mail Address Definition** window.
- 2 Enter the e-mail address in the **E-mail Address** field.
- 3 If you want to attach this address with a cardholder record select the option Associate with a Cardholder.
- 4 Using the expand button select the cardholder record you want to attach with the address.
- 5 Click **Save and New** to save the current record and define a new one. Choose **Save and Close** to save the current record and close the window. Select **Close** to close the window without saving the record.

Mass Insert

The second method of storing e-mail addresses is via Mass Insert option. This method provides you the option to store multiple e-mail addresses at the same time. If you are using this method "Associate with a Cardholder" option will not be available while defining the addresses.

The Cardholder Definition program provide you an option to link the cardholder record with the e-mail addresses you have defined here.

- 1 Select **File>Insert E-mail Addresses**.
- 2 Enter the data in the **Insert E-mail Addresses** window.
- 3 Click **OK**.

Editing records

- 1 To edit an e-mail address you have defined, select the record by a left mouse click and double click on it. You can also use the edit icon located on the tool bar. The **E-mail Address Definition** window displays the record you defined. Make your changes and click **Save and Close**.

Deleting records

- 1 To delete an e-mail addresses, select it by a left mouse click and choose the - (minus) icon from the tool bar.

Search

When you click on the binocular icon, the E-Mail Address Search Wizard is activated. To view the entire e-mail address database, press the **Find Now** button without entering a value in any field. *The default search order is displayed alphabetically.* To find particular records enter the value in the empty field and click **Find Now**.

To change the sort order, left click on a column heading. For instance, to sort by Cardholder ID, click on the Cardholder ID title bar.

The size and order of columns can be changed by dragging and dropping to a new location. The bottom left corner of the screen displays the number of records that have been selected

Advanced Find

Using **Advanced Find** feature, you can build the search criteria by selecting appropriate entries from the drop down list box and entering specific value in the value field. You have to select a specific field name, condition and a specific search value.

Advance Find feature uses Boolean logic to create complex and highly precise searches. Boolean logic uses three connecting operators (NOT, AND OR) to narrow or broaden a search or exclude a term from the search. It is the process of linking criteria to narrow or expand a search through the use of **NOT, AND** or **OR**.

The Advance Find feature helps the operator to customize the search function. The operator can define the searches and save them for later use.

The saved search criterion is displayed only for the operator who defined it. The e-mail addresses can be searched using e-mail address and cardholder fields (like first name, last name etc.).

- 1 Click on the **Advance Find** tab located on the top of the **Search** window.
- 2 The **Advance Find** window opens.
 - a) Define your search criteria.
 - b) If you want to search for E-mail ID = 10, you need first select the left parenthesis from the list box. Parenthesis can be used to create nested search clauses. Using the Parenthesis one can override the standard order of priority (left to right) for each Boolean statement in the search.
 - c) Select E-mail ID as the Field Name.
 - d) Select equal to (=) as the condition.
 - e) Enter the value as 10.
 - f) Provide the closing parenthesis at the end.
 - g) When you are satisfied with the criterion, click **Add to List** button. If the criterion is not valid, it is displayed in red under the Where Clause section. When the criteria becomes valid the font color changes to black.
 - h) If you want to specify additional search condition you can select AND/OR from the list box.

UDF Cross Reference

CHAPTER 12

Introduction

The **User Defined Field Cross Reference** (UDF Cross Reference) makes it possible to map a User Defined Field (UDF) with a badge technology and a badge layout. This program works in conjunction with the Cardholder Definition program. UDF Cross Reference helps the user to create badges automatically. This feature becomes more useful to the users and saves lot of time and effort when you create large number of badges with the same badge layout and technology.

Accessing the application

- 1 Open the launcher by double clicking on the launcher icon on your desktop or go to Start>Programs>Schlage SMS>Schlage SMS.
- 2 In the login window, enter your assigned user ID and password.
- 3 In the System Launcher window, double click on UDF Cross Reference icon.

Working with UDF Cross Reference

Before you begin

In order to work with this program you need to meet the following pre-requisites.

- 1 First, you need to create required badge layouts and annotations depending on the need of your company.

- 2 Create a user defined field using **User Defined Field Editor (UDF Editor)**. Verify that the field appears correctly in the **Cardholder Definition** module. For instance create a required, string field called “Badge Link”.

The screenshot shows the 'Cardholder Definition' window. The 'Last Name' field is highlighted with a blue selection box. The 'First Name' field contains 'Kate'. The 'Initial' field is empty. The 'Notes' field is empty. The 'Activation Date' is '2/27/2007' and the 'Expiration Date' is '12/31/2199'. The 'Cardholder ID' is '3'. The 'Access Blocked' checkbox is unchecked, 'Controlled Antipassback' is checked, and 'Special Access Privileges' is unchecked. The 'Image Capture Date (UTC)' is '2/27/2007' and the 'Signature Capture Date (UTC)' is '2/27/2007'. The 'Badge Link' field is empty. Below the form is a table with the following data:

Credential ID	Stamped ID	Encoded ID	Issue Code	Keypad ID	Back
2	56565	45465465	1	0	

At the bottom left, it says '1 Online Credential'. On the right side, there is a 'Portrait' section with a photo of a woman and a 'Signature' section with a handwritten signature.

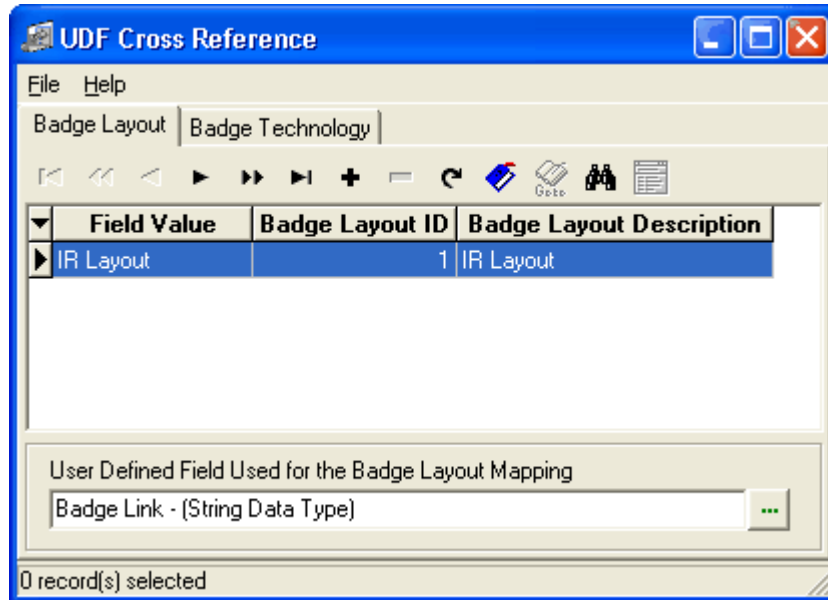
Note: While inserting a new mapping record, the program will determine what type of field is the UDF; whether it is an integer or a string. The program allows only valid values. If the UDF is an integer you can only add numeric data in the field value. You cannot enter alphanumeric data. If you try to change an existing UDF, from string to an integer, you will get a warning message saying that all the records with field values that are not integers will be deleted.

- 3 In **System Settings** under the **Badge Options and Pin Calculator** section select the following options.
 - Enter Encoded ID and Stamped ID Later
 - Auto Generate Stamped ID
 - Badge Insert Partial Automation Mode

Mapping

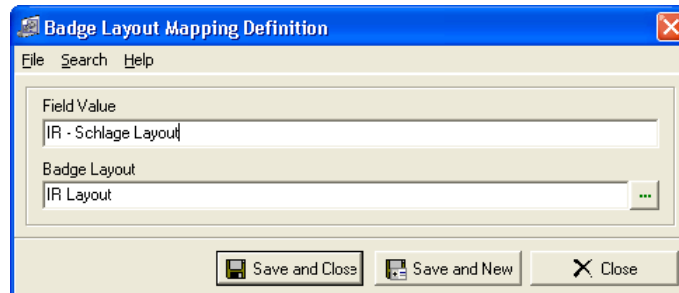
- 1 Open the **UDF Cross Reference** program through the **System Launcher**.
- 2 The program window is displayed.

Note: You need only one user defined field to map with both badge layout and badge technology. At the same time you can create as many links as you like by using different field values.



Note: The grids have all the same functionality as the rest of the Schlage SMS programs. Add, Delete, Edit, Refresh and Find work exactly the same.

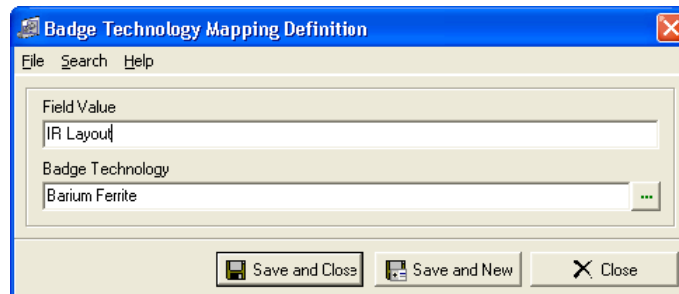
- 3 Click the plus sign (+) to define the mapping. The **Badge Layout Mapping Definition** window is displayed.



- 4 Enter a **Field Value**. Select a **Badge Layout**.
- 5 This field value will correspond to the badge layout you have selected here. You can define as many mappings as you wish, but there cannot be duplicate field values. Click **Save and Close** to complete the badge layout mapping or click **Save and New** to define a new mapping.

Note: In order for the UDF Cross Reference to work, you need to enter same field values in the Badge Layout Mapping Definition and in UDF field in the cardholder record.

- 6 On the **UDF Cross Reference** window, select the user defined field for badge technology mapping. Click the **Badge Technology** button. Click the plus sign (+) to define a badge technology mapping.



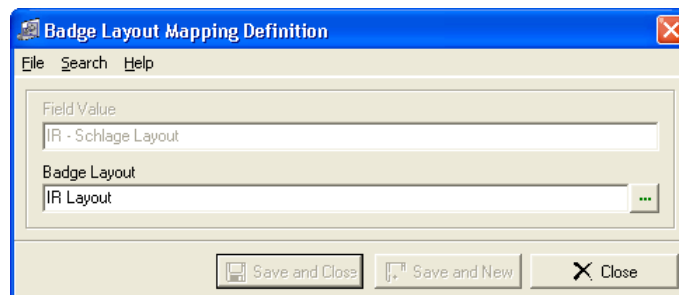
- 7 Enter the same column value, which you used for badge layout. Select the badge technology. Click **Save and Close**.
- 8 On the **UDF Cross Reference** window, select the UDF used for badge technology mapping. This field is located on the bottom left corner of the **UDF Cross Reference** window. This user defined field must match the UDF that you selected for the badge layout mapping.
- 9 Close the **UDF Cross Reference** program and open the Cardholder Definition program. Open a cardholder record. When you click **Add Badge** you can see that a blank badge (a badge without a stamped ID or encoded ID) is created. You are informed with a summary window, which shows the cardholder information and badge information.

Note: You can add encoded ID and stamped ID later.

- 10 In **System Settings**, if you have selected the above mentioned options (*See Step 3 in Before you Begin*) when you create a credential for a cardholder, the badge layout and badge technology are automatically populated.

Editing an Existing Mapping

- 1 When editing an existing mapping, the field value cannot be changed. You can only edit the badge layout field and badge technology fields.



Note: The field value option is disabled which means you cannot edit that field.

Two Person Rule

CHAPTER 13

Two Person Rule functionality provides the user with tools for defining the access control criteria for areas that can be accessed only by two or more persons at the same time. Access to these areas can be gained only if the minimum occupancy count is satisfied. The system tracks the occupancy count for such areas and generates appropriate alerts if a violation is detected.

Also, the system allows the user to dynamically monitor the current occupancy status of the Two Person Rule areas. The system displays all the details of the current occupants. The user is able to reset the occupancy count of these areas and the system keeps track of any reset.

In highly secured areas like vaults, the assignment of workers is based on teams. The system allows creation of teams, and workers are assigned to these teams as team members. Only members of these teams can have access to these areas. For additional security, when the area is not empty, there must be at least two people from different teams in the team controlled area.

Supervisors can gain access to two person rule areas only after presenting their credential and receiving final approval via a push-button from a worker within the cash room.

Note: The reader interface must have firmware version FTW_09.hex, in order for the team members to gain access to the two person rule areas.

Area Definition

The first step in securing an area with two person rule feature is defining an area. You can define three different types of areas. One is the normal area, the second one the Two Person Area- Scheduled, and the third one is the Two Person Area- Team. As the name suggests, a **Normal** area provides access to the normal areas. In that case there is no need to specify a minimum or maximum occupancy count.

If the area is marked as **Two Person Area - Scheduled** the access is given to a certain group of people using the Team Definition module (discussed later in this chapter). The number of people occupying the area type Two Person Area - Scheduled must be at least two and no more than maximum number specified (maximum occupancy count). If the area is currently empty, the first two cardholders entering the area must present their credentials within fifteen (15) seconds interval.

If the current occupancy count is greater than or equal to two (minimum occupancy count), another cardholder who has access can enter the area using a single card swipe. If the current occupancy count is two, to gain a valid exit transaction, the two members should present their credentials within fifteen (15) seconds. The Two person rule area can also be empty.

In the case of **Two Person Area - Team**, you need to define two teams (using the Team Definition module) and assign cardholders to each teams. Only members of these teams will have access to these areas. When the area is empty, the access is allowed only if the persons who are trying to access the area are from two different teams. If the current occupancy count is at least two, the other members of the teams are allowed to enter the room regardless of the fact that they are from the same team or two different teams. When the area is not empty, at least one person from each team must be present in the area.

Define Readers

The next step is to define the reader that give access to these areas. All readers must be defined as standard readers even though there a pair of readers are required for every TPR area – one on entry and one on exit. For the “exit” readers, the egress two person rule area (the area that the cardholder is leaving behind) must be defined.

Note: In order for the system to function properly the readers must have FTW_09.HEX firmware. Otherwise the transaction monitor may show duplicate transactions for single card swipe.

Follow these steps to define a reader that gives access to a two person rule area.

- 1 Open **System Manager>Hardware Map>Edit Readers**.
- 2 Select the insert button (+) from the grid.
- 3 The **Reader Definition** window opens.
- 4 Enter a description and notes attached to it.
- 5 Select the controller that this reader is attached to.
- 6 Next, select the two person rule area this reader is providing access.
- 7 Select the reader model from the pop-up window.
- 8 **Antipassback Time** - N/A This is implemented through firmware.
- 9 Select the **Channel Number** and **Reader Address**.
- 10 Select the **Reader Template**. To add a reader as a template, choose **Reader Templates** from the **Edit** menu of the main window.

Note: Further information on Reader Templates is available in **System Manager** section.

- 11 Select the option **Installed**. If this option is not selected the reader will not function as required.

- 12 Select **Save and Close** to save the record and exit the Reader Definition window. Select **Save and New** to save the current record and create a new one. Select **Close** to simply close the window without saving the record.

The screenshot shows the 'Reader Definition' window. The 'Description' field is filled with 'Development Room'. The 'Attached To' field shows 'SRCNX - 16'. The 'Provides Access To Area' field shows 'Development Room'. The 'Reader Model' field shows 'SRINX - 1 RELAY'. The 'Reader Type' field shows 'Standard Reader' and the 'Door Type' field shows 'Pedestrian'. The 'Antipassback Time (Minutes)' is set to 0, 'Channel Number' is 1, and 'Reader Address' is 1. The 'Reader Template' is 'No Template'. In the bottom section, the 'Installed' checkbox is checked, and the 'Degraded Mode' checkbox is also checked. The 'Auto Relock' checkbox is unchecked. The bottom of the window features three buttons: 'Save and Close', 'Save and New', and 'Close'.

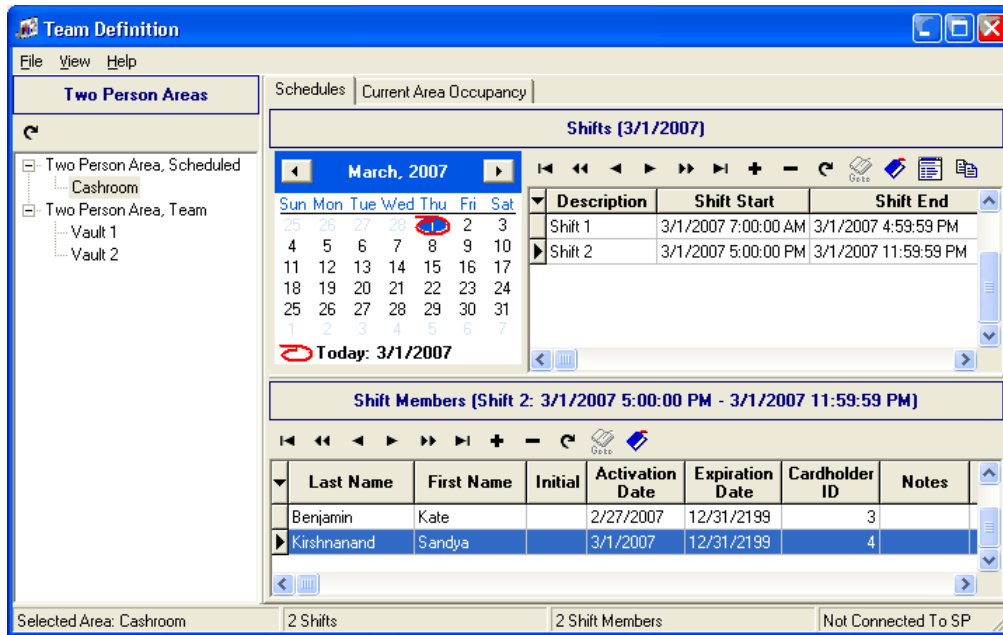
- 13 Follow these steps to define a normal reader with a two person rule area as the egress area.
- 14 Follow steps 1 to 5 from the previous section.
- 15 Now select the area this reader is providing access. In this case the reader is functioning as an **Exit Reader** for the two person rule area. So the area the reader is providing access may be a hallway.
- 16 Next select the Egress Area check box. Select an egress area from the pop-up window. It must be a two person rule area since an egress area is what the cardholder is leaving behind. All other options are same as the previous section. Make appropriate changes.

Team Definition

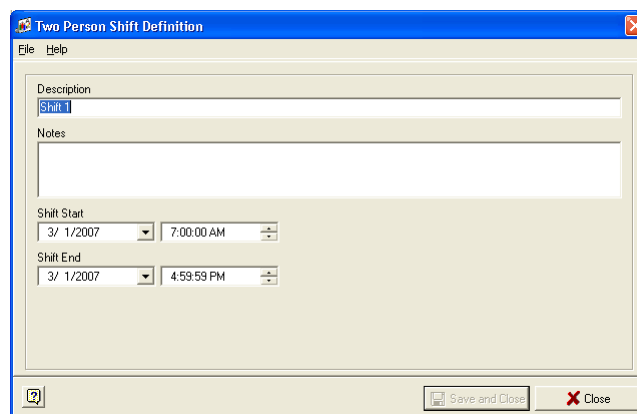
The shifts and the teams for the two person rule area is defined using the Team Definition module. The team definition application displays the two person areas that have been defined as team access or scheduled access. If the user selects the "two person area – scheduled" option the system allows defining a shift and assign start and end times for the shift. If the user selects the "two person area – team" option the system displays two groups (group A & group B). The user can select a cardholder from the available cardholders who have been created using the Cardholder Definition application. The system allows the user to assign the cardholders to shifts or teams based on whether the selected area is a "two person area – schedule" or "two person area – team".

Creating a Shift

- 1 Open the **Team Definition** application from the **System Launcher**.



- 2 Left side panel shows all the two person areas divided into two groups:
 - Two Person Area, Scheduled
 - Two Person Area, Team
- 3 Select an area from the **Two Person Area, Scheduled section**. The Schedules tab is active now. The upper part of the window shows the shifts and the lower section displays the shift members.
- 4 To define a new shift, click on the insert button (+) from the **Shifts** section of the main window.



- a) Enter a description for the shift.
- b) Enter the notes related to it
- c) Specify a **Shift Start** date and time.

- d) Specify a **Shift End** date and time. Every shift defaults to current day and ends after 24 hours. You can change it manually by selecting a different date and time.

Note: The calendar helps the user to select multiple days for the shift. To select multiple dates in the calendar, place your mouse pointer on a date, depress the mouse button and slide the mouse over the dates you want to select. Do not release the mouse button until you have selected the dates.

- e) Now add the shift members to the shift. Select the Shift Members tab that appears on the **Two Person Shift Definition** window. Click on the insert button (+) to add new cardholders. The search window displays cardholders with only one badge. Select the cardholders you want to add to this shift and click OK. The selected cardholder records appear on the shift members section of the **Two Person Shift Definition** window.
- f) Select **Save and Close** to save the record and exit the Two Person Shift Definition window. Select **Save and New** to save the current record and create a new one. Select **Close** to simply close the window without saving the record.

Note: Shift members can be added also using the insert button on the lower section of the Team Definition window.

Duplicating Shifts

The Team Definition module allows the users to duplicate the shifts easily.

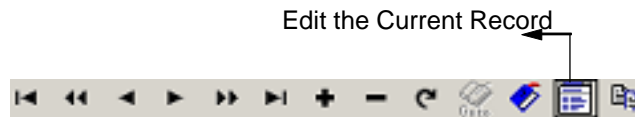
- 1 To duplicate a shift, first select the shift you want to duplicate and click on the **Duplicate the Selected Record** button from the tool bar of the Team Definition window.



- 2 The **Duplicate Shifts** window provides the following options.
 - a) **Duplicate Shift Time Only** - Select this option to create a copy of the shift time only into another day or days. The description of the shift is also copied. The members of the original shift are not duplicated. The destination area or areas have to be specified (can be the same area).
 - b) **Duplicate Shift Start Date** - Specify a shift start date. The shift end date is duplicated.
 - c) **Duplicate Shift Start Date** - Specify a shift end date. The shift end time is duplicated.
 - d) **Duplicate Shift Date and Time** - Selecting this option creates a copy of the shift (days, time and, optionally members). The destination area or areas have to be specified. The source area can also be a destination area – in this case the exact copy will be created. The name of the shift will be copied.
 - e) **Duplicate Shift Members** - The members of the original shift are copied only when this option is checked.
 - f) **Areas to Duplicate Shifts** - Once you have selected the appropriate duplicate option, click on the insert icon under the section Areas to Duplicate Shifts to add the areas for which this shift is created. The pop-up window displays all the **Two Person Area - Scheduled** records.
 - g) Click **OK**.

Editing Shifts

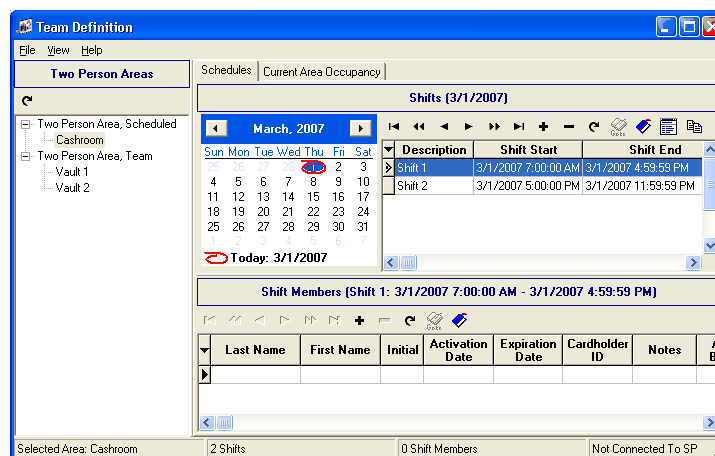
- 1 To edit a shift, select the area, select the shift and click on the **Edit the Current Record** button or double click on the record.



- 2 The **Two Person Shift Definition** window opens.
- 3 Make appropriate changes and select **Save and Close**.
- 4 Shift members can be modified using the delete and insert buttons on the tool bar located on the **Shift Members** section of the **Team Definition** window.

Creating Teams

If the user selects an area that is two person area – team, the Team Definition window displays two groups (group A & group B). The user can select a cardholder from the available cardholders who have been created using the Cardholder Definition program.



- 1 To add members to the groups (teams), select the section **Two Person Area- Team**. To add members to Group A, click the Edit button from the tool bar or select **File>Edit Teams**.
- 2 The **Team Member Definition** window displays two sections. The upper part of the window shows the Teams and the lower section displays the team members. To add members to Group A and Group B, select a group and click the **Insert a new record** button (+) from the **Team Members** section of the Team Member Definition window.

Note: The members added to Group A and Group B (teams) will have access to all the areas comes under the category Two Person Area-Team. The modifications made to the area records in the System Manager can be viewed in Team Definition by clicking the Refresh button located on the left hand side of the Team Definition window. The access records created in Team Definition can be viewed in System Manager and Cardholder Definition. They cannot be edited or deleted from there though.

View Cardholder Images

- 1 To view a cardholder's portrait or signature, select the cardholder record and choose **View>Cardholder Images**.

Area Count Tracking

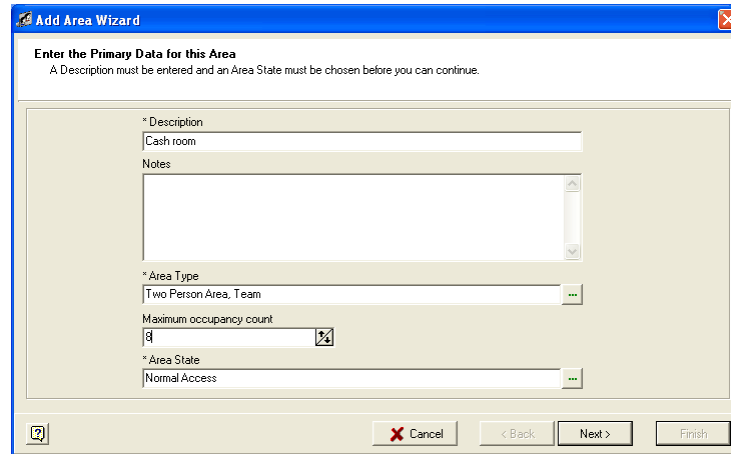
The Two Person Rule feature provides area occupancy count tracking. The system maintains a count of cardholders within each area based on the entry/exit card swipes from that cardholder. Occupancy count override functionality allows the administrator to reset the count for any area and set it to zero (0). Occupancy status allows a dynamic view of current area occupancy including the names of the current occupants to that area. However, if a supervisor is present in the Two Person rule Area, his/her presence does not count towards the minimum occupancy count.

- 1 To view the occupancy count for an area, select an area and click the **Current Area Occupancy** tab located on the Team Definition window.

Define a Two Person Area - Schedules or Team

- 1 Login to **Schlage SMS**.
- 2 Go to **System Manager>Areas>All Areas**. (see "Areas and Area Sets" on page 75)
- 3 In the Grid section of the **System Manager** window, the All Areas tab is enabled. Click on the **Insert (+)** button. The **Add Area Wizard** opens.
 - a) Enter the primary information for the area.
 - b) Enter a **Description** for the area. You can enter maximum sixty four (64) characters.
 - c) Enter the **Notes** related to it. The maximum characters allowed is two hundred and fifty (250).
 - d) Select the **Area Type**. As described above there are three choices. Normal, Two Person Area, Scheduled and Two Person Area - Team. Since you are defining a two person rule area, the first choice (normal) does not apply.
 - e) Specify the maximum occupancy count for the area. If the occupancy count reaches the maximum for an area, the system denies access and generates a two person rule violation transaction. The maximum number you can set is sixty four (64).

- f) Select the Area State from the pop-up window.



- g) Click **Next** to continue.
- h) The options shown in this page does not apply to a two person rule area.
- i) Next select the Area Set that this Area may be a part of.
- j) Click **Finish** to save the record.

Supervisor Access

Supervisors can gain access to Two person rule areas only after presenting their credential and receiving final approval via a push-button from a worker within the Two person rule area. In order for the supervisor to gain access to these areas the current occupancy of the area must be at least two. The following are the procedure that gives supervisors access a Two person rule area.

- 1 Supervisor presents the credential.
- 2 The system notifies the occupants of the request for access by the supervisor by turning the strobe light on.
- 3 One of the occupants acknowledges the request and grants access by pressing a push button.
- 4 The occupancy count is not updated.

Portrait Monitor-Settings

CHAPTER 14

Introduction

In the Schlage SMS, the cardholder activity and the images are viewed in real time on the computer monitors using the Portrait Monitor. The **Portrait Monitor Control** program determines the settings and features that are enabled in the Portrait Monitor module. Device, time zone, workstations and the option to view images are configured here.

Note: This is a control module. Therefore a user must be granted **Read/Write** permissions to this program in the **System Security**. It is recommended that only Schlage SMS administrators be granted permission to this application.

Overview

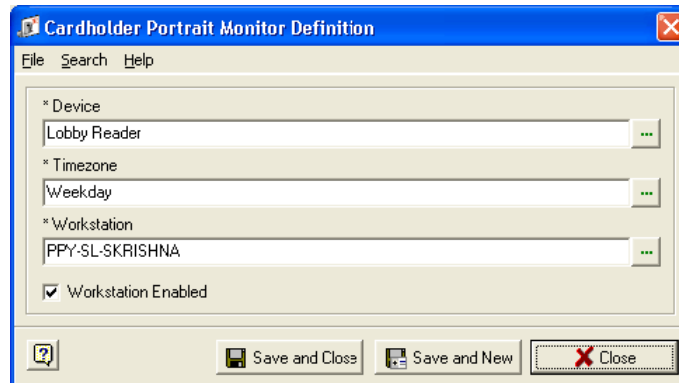
To view a portrait using **Portrait Monitor** program, a computer must be designated to receive and display information. The tool bar offers a variety of icons for add, delete, refresh, bookmark and edit functionalities. The different arrows allow you to move between the records quickly. Configuration requires the selection of a device (reader), time zone and workstation ID.

Accessing the Application

- 1 Go to **Start>Programs>Schlage SMS>Schlage SMS** or open the System Launcher by double clicking on the Launcher icon on your desktop.
- 2 Enter your assigned Used ID and Password into the Login window.
- 3 Select the **Portrait Monitor Control** icon from the **System Launcher** window.

Configuring a Portrait Monitor Workstation

- 1 To designate a computer as a Portrait Monitor Workstation, select the + icon on the main window tool bar to activate the Cardholder Portrait Definition window. Device, Time zone and Workstation ID are required fields. The expand button opens the various selection windows for each of the fields.



- a) **Device** - Opens the Reader Selection window that is used to define the device to be monitored.
- b) **Timezone** - Allows a time zone selection for the workstation. The workstation will only act as a Monitor station during the hours defined in the time zone applied to it.
- c) **Workstation** - Defines the workstation(s) that will monitor devices, cardholders and their transactions.
- d) **Workstation Enabled** - Place a checkmark in the box to enable Portrait Monitor on the workstation that is selected. If this option is not checked, the workstation will be disabled and the Portrait Monitor will not display any pictures. The default is off.
- e) Click **Save and Close** exits the application window once your selections are complete. You can now view the records in the main window. Click **Save and New** to configure another workstation and device. If you click **Close** a confirmation message pops up and gives you the option of either canceling or saving the record.

Portrait Monitor Search Wizard

- 1 Open the search dialog by clicking on the binoculars.

Note: Enter the search word in the search criteria field and click Find Now.

- 2 The search result shows all the records corresponding to the search entry.

Note: The system puts a * (wild card) after the search entry and search returns all the fields with the search criteria.

The Advanced Find button located on the top right hand corner of the Search window helps the user to run a more specific search.

Advanced Find

Using Advanced Find, you can build the search criteria by selecting appropriate entries from the drop down list box and entering specific value in the value field. You have to select a specific field name, condition and a specific search value.

Advanced Find feature uses Boolean logic to create complex and highly precise searches. Boolean logic uses three connecting operators (NOT, AND OR) to narrow or broaden a search or exclude a term from the search. The Advance Find feature helps the operator to customize the search function. The operator can define the searches and save them for a later use. The saved search criteria is displayed only to the operator who defined it.

- 1 Click on the **Advance Find** tab located on the top of the Search window.
- 2 Define your search criteria in the following window.
- 3 Define the criteria you want to use.
 - a) If you want to search for Device Control ID=10, you need to first select left parenthesis from the list box.
 - b) Parenthesis can be used to create nested search clauses. Using the parenthesis, one can override the standard order of priority (left to right) for each Boolean statement in the search.
 - c) Select Device Control ID as the Field Name.
 - d) Select equal to (=) as the condition.
 - e) Enter the value as 10.
 - f) Provide the closing parenthesis at the end.
 - g) If you would like to specify additional search condition you can select AND/OR from the list box.
 - h) If you enable the NOT check box the search result will display all the records except the ones mentioned in the NOT search criterion.

E.g. If you want to search Display Control IDs less than or equal to 3 with Proximity Reader as the device to be monitored or Display Control IDs greater than or equal to 25 with Main Door Reader as the device, you can define the search criteria as follows.

(([Display Control ID] <= 3) AND ([Device] = proximity reader)) OR (([Display Control ID] >= 25) AND ([Device] = Main Door Reader))

Note: While searching for a string you can put a % (wild card) before and after the search entry. The search returns all the fields with the search criteria. For example if you search for a device called %Proximity Reader% the search returns all the records contain the word "Proximity Reader".

Portrait Monitor

CHAPTER 15

Introduction

The Schlage SMS offers another type of reporting tool, the **Portrait Monitor** module. Activity and images are viewed instantaneously on any designated computer monitor. This application can be used to validate and track cardholder identity and access. Detailed information with cardholder or guest images is examined as the transaction occurs. Assigning workstations as portrait monitors is accomplished in the **Portrait Monitor Control** module.

Starting the Portrait Monitor

This module can be added to the **Start up** tab in the **System Security** program for each workstation that is to receive alarms.

- 1 To do this, go to **System Security\Startup**, click **Add** and select Portrait Monitor.

Note: Remember to give proper privileges (at least Read-Only rights) to the users of Portrait Monitors or they will not be able to use the program.

You can also open the program from the **System Launcher** window.

- 2 Open the **Launcher** by double clicking the Launcher icon on your desktop.
- 3 The login window opens. Enter your user ID and password.
- 4 In the **System Launcher** window, double click on **Portrait Monitor** icon.

Working with Portrait Monitor

The main screen components of the application are the menu bar, the image view section to the left, the details information display to the right (on by default) and manual override and details buttons at bottom left.



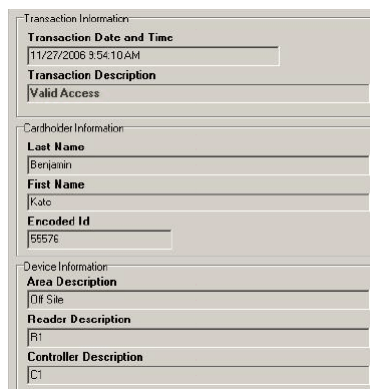
Launching the Portrait Monitor

- 1 Select **View>Popup Enabled** option to launch a minimized Portrait Monitor screen when a transaction occurs.

Detail View

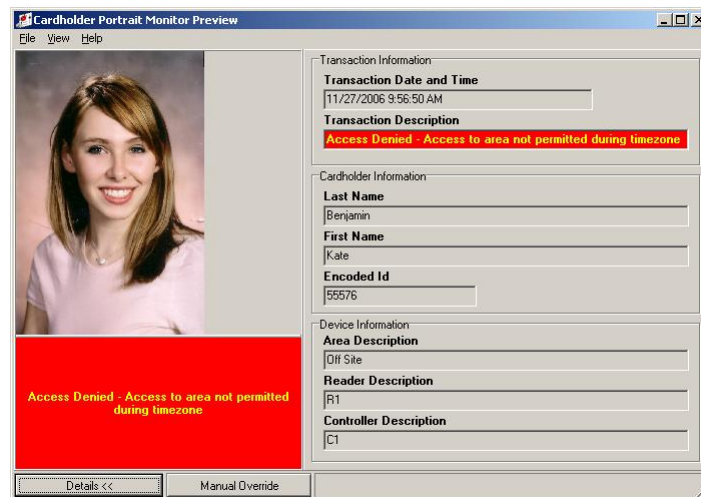
The **Details** section displays the transaction information, cardholder information, and the device information.

Select **View>Details** to turn on the detail information section (on by default). When **View>Details** is unchecked only the **Image View** (cardholder's portrait view) is active and therefore no transaction, cardholder or device information is seen. The Details button at the bottom functions in the same way.



Access Denied Transactions

In the Portrait Monitor, Access Denied transactions are displayed in red color. When an access denied transaction occurs, a red panel displays underneath the image stating the transaction. The user can resize this field to their convenience and it will save to the User Registry when the program is next opened.



Pausing Transactions

Select **View>Pause** to halt the application temporarily from displaying any new transaction. The information that was on the screen at the time that **Pause** option was selected will remain.

Manual Overrides within Portrait Monitor

Clicking **Manual Override** located at the bottom of the Portrait Monitor window opens the main window of the Manual Override module. Provided that the operator has at least *Read Only* rights to the Manual Override module, he can execute a device override. Highlight the task and select the Execute Override Task button. Please refer to the **Manual Override chapter** for further information on this module.

Alarm Definition

CHAPTER 16

Introduction

This chapter describes how alarms are initially programmed and configured in the system. An alarm definition requires the configuration of transactions, workstations, devices, cardholders, time zones etc.

Concept behind alarms

When a transaction occurs, the SP takes the transaction information and searches for transactions defined as alarms. Once the SP finds an alarm label, it generates the alarm. The SP then retrieves the alarm label information to get the groups and workstations that are attached with the alarm. Once the SP finds the workstations, it sends the alarms to specific workstations.

There are six alarm types defined in the **Schlage SMS**. They are card, contact, communications, controller, operator and system Alarms. Most system activities such as status messages, communication failures and other transactions may be alarmed. An example of a communication alarm would be *"a lost link to a reader"*. An *expired badge* is a card alarm condition.

Multiple workstations can receive alarms simultaneously or they can be rerouted in sequence. An alarm can be directed to a specific user, regardless of where he or she has logged in, through the association with a group and the workstations attached to that group. Alarms can be prioritized to ensure immediate notification of the most important alarms and can be customized to appear in a specific scheme of colors.

Accessing the application

- 1 Open the System Launcher by double clicking on the desktop short cut or select **Start>Programs>Schlage SMS>Schlage SMS**.
- 2 Login to the system using your assigned user ID and password.
- 3 Double click on the **Alarm Definition** icon in the launcher window. This will open the Alarm Definition module.

Defining Alarms

In **Schlage SMS**, alarms are defined using **Alarm Definition** module. The purpose of the Alarm Definition module is to define certain transactions as alarms and associate them with Security Groups and Workstation Attachments. The three sections of the Alarm Definition program are Label Definition, Group Attachment and Alarm Attachments.

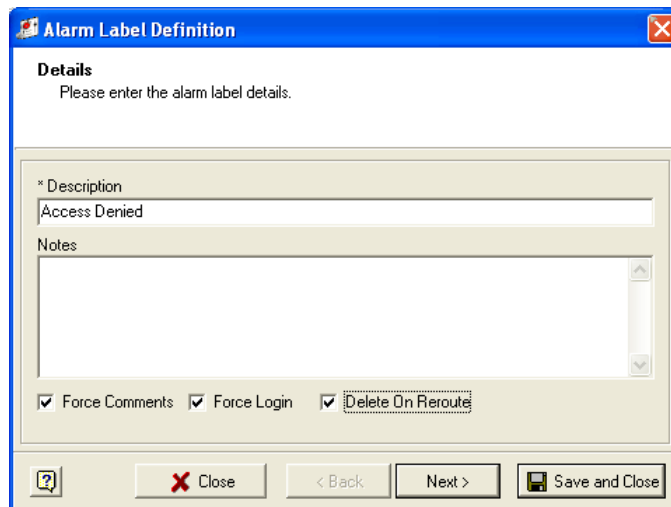
Alarm Label Definition

Alarm Label is used to give an alarm a name (or label) by clicking on icon. Description, notes, operator instructions, acknowledgment requirements, re-route settings, and workstation display colors are defined in this section.

The user can also attach .wav files (i.e. sound file) with the instructions. The new version of software also allows the user to add unlimited number instructions along with the label.

Adding an Alarm Label

- 1 To add a new **Alarm Label**, click on the icon under the Label Definition section and it opens the **Alarm Label Definition** window.

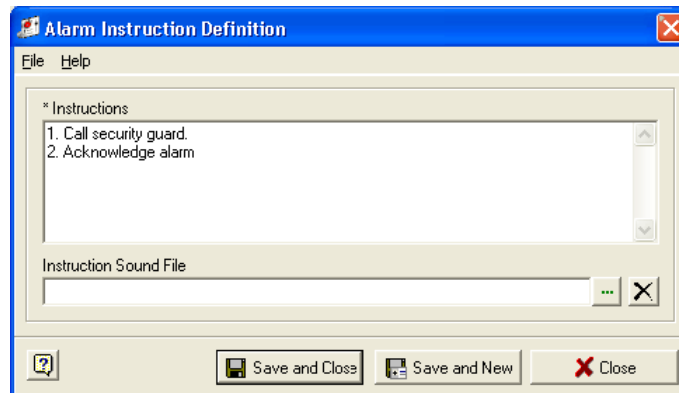


- 2 Enter the description (type) of the alarm, notes, instructions and acknowledgement requirements (for the operator receiving the alarm). The description will appear in the left column of the main screen.

Acknowledgement requirement fields:

- **Force Comments** - When checked, the operator must type or insert a comment in order to acknowledge an alarm.
- **Force Login** - When checked, the operator must type their user ID and Password in order to acknowledge an alarm.

- **Delete on Reroute** - If selected, when the alarm acknowledgement time expires, the alarm is removed from the current workstation and rerouted to appear only at the next workstation in the group sequence. If you don't choose this option, the alarm will remain on each workstation it is routed to, until it is acknowledged.
- 3 Click **Next** to continue the alarm label definition.
 - 4 Next, enter the instructions for the operator while acknowledging the alarm. The user can enter an unlimited number of instructions with each alarm label.
 - a) The user can also associate .wav files (sound files) with the instructions.
 - b) Click on the + sign located on the upper side of the window. Enter the instructions and attach the sound file.

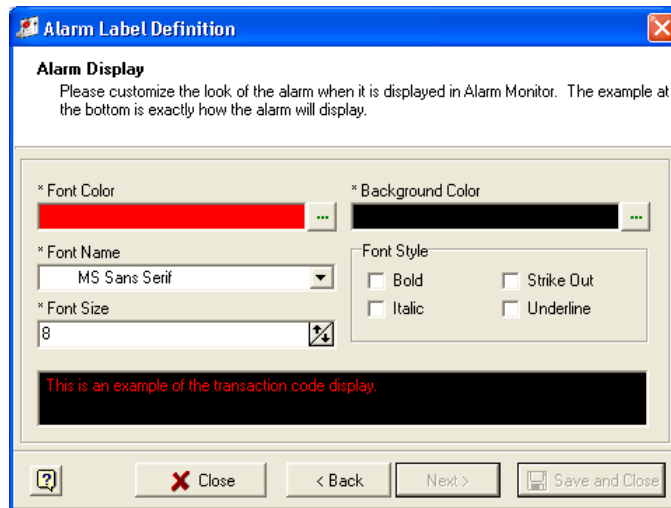


- c) Click **Save and New** to enter a new set of instructions or click **Save and Close** to save and close the window.
- 5 Next, choose different .wav files for different alarm states. If you don't want to have sound files with instructions you can skip this section by clicking the **Next** button. The user can also specify the time interval for looping the sound file.



- 6 Click the play button to play the sound file. Click **Next** to continue. When an alarm occurs, the Alarm Monitor or Alarm Graphics program will play the sound file attached with the alarm. Depending on the state of the alarm, the system will choose the right file and plays it.

- Next, customize the appearance of alarms. The user can select font name, color, size, style and background color.



- Once you are satisfied with the alarm display, click **Save and Close**. You can see the preview of the display in the bottom of the window.

Editing an Alarm Label

The user can edit any previously entered information by using the edit feature. Double click on the record you want to edit and it opens the edit window with the details associated with the label i.e. instructions, display settings etc.

- Click on the corresponding buttons to edit that field. Click **Save and Close** to save the changes that you made.

Group Attachments

Group attachment is used to add new groups, copy existing groups to alarm labels, set group time zones, alarm priority, acknowledgment times and to attach workstations to groups.

Creating Group Attachments

Now that the Alarm Label has been set up you must create an **Alarm Group**. At the bottom of the Alarm Definition window you will see two tabs: **Group Attachment** and **Alarm Attachment**.

- Before beginning you must first select an **Alarm Label** by clicking in the Selected field of the Alarm Label.
- Now click on the **Group Attachment** tab and then click on the icon on the tool bar or the **Add Group** button to the bottom right of the tab.
- The **Group Attachment Definition** window opens.

Adding a new group

- To add new groups click on the icon in the **Groups** section of the **Group Attachment Definition**. The Group Definition window is enabled. Fill in the Description (name) and Notes fields.

- 2 Choose **Save and Close** or **Save and New** if you want to add the next record. The new Group will be listed in the main Group Attachment Definition window.

Adding Workstations

The next step is to add Workstations, Alarm Operators and/or E-Mail Recipients to your Groups. To do this, you will need to define Alarm Operators and E-Mail recipients, as well as choosing from existing physical workstations in the database.

Workstations, alarm operators and email recipients

The following section gives details about setting up workstations, alarm operators, email recipients.

Workstations

- 1 When you click on the button in the **Group Attachment Definition** window, **All Workstations** window opens listing all the workstations that have been defined. If you have not defined any workstations, define them by clicking the + button on the top of the **All Workstations** window.
- 2 Once you have defined all the workstation, select your group, select the workstation(s) to be attached to this group and click on **Copy to Groups** at the bottom.
- 3 A confirmation message appears. Click **Yes** to continue.
- 4 You can attach as many workstations to a group as needed. You will be prompted to confirm and then can close this window to return to the **Group Attachment Definition** window.

User Alarm Workstation

- 1 To define **Alarm Operators**, click on the + icon in the **All Workstations** window. The Workstation Definition window will open. Select **User Alarm Workstation**.

- 2 Next, click on the expand button to open the **Select an Operator** screen. All operators defined in the System Security module will be listed here. Highlight your selections and click **OK**.
- 3 Select a holiday set and the locale timezone for this workstation. Remember to select the appropriate Holiday Set and Time zone based on the physical location of the operator to which you are sending alarms.

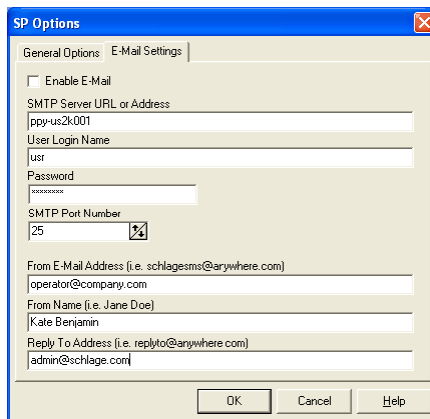
- 4 Save your changes when all remaining field selections are completed. The All Workstations screen will now display Operators as User Alarm Workstations in the **Workstation Type** column.

E-Mail Recipient

System Processor Setup

The setup for **Alarm E-Mails** must be completed first. The SMTP (Simple Mail Transport Protocol) server settings required for this feature

- 1 From System Processor, choose **File->Edit Options** and then click on the tab for **E-Mail Settings**.

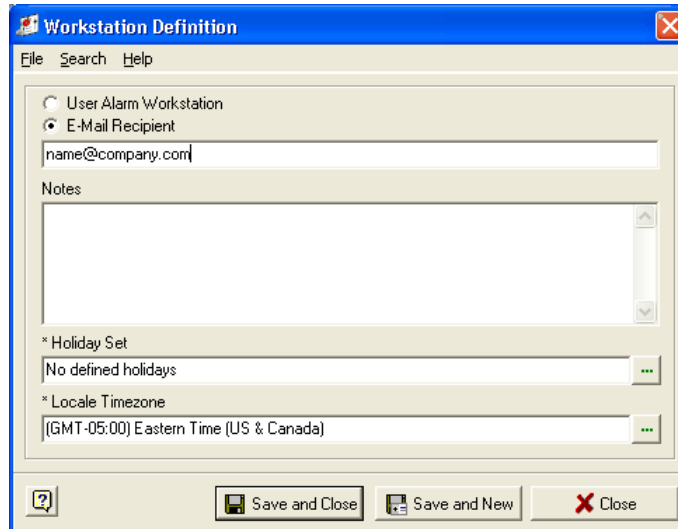


The screenshot shows the 'SP Options' dialog box with the 'E-Mail Settings' tab selected. The 'Enable E-Mail' checkbox is unchecked. The 'SMTP Server URL or Address' field contains 'ppp-us2k001'. The 'User Login Name' field contains 'usr'. The 'Password' field is masked with 'xxxxxxxx'. The 'SMTP Port Number' is set to '25'. The 'From E-Mail Address (i.e. schlage@anywhere.com)' field contains 'operator@company.com'. The 'From Name (i.e. Jane Doe)' field contains 'Kate Benjamin'. The 'Reply To Address (i.e. replyto@anywhere.com)' field contains 'admin@schlage.com'. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

- a) **Enable E-Mail:** If this is checked, E-mailing alarms is turned on globally. If it is not checked, E-mail is disabled globally, regardless of any E-mail workstations entered within Workstation Definitions.
- b) **SMTP Server URL or Address:** The IP Address or URL of the SMTP Server. This host name can be any valid SMTP server with the capability of supporting standard SMTP mail formats.
- c) **User Login Name:** The login name to the SMTP server.
- d) **Password:** Enter the password to the SMTP Server.
- e) **SMTP Port Number:** The industry standard port number for SMTP Server. Usually it is port 25.
- f) **From E-Mail Address:** The address typed here will be displayed in the 'From' area of the E-mail that is generated.
- g) **From Name:** The name that will appear on the E-mail that is generated.
- h) **Reply To Address:** If a reply is made to the E-mail that is generated by the System Processor, this E-mail address will appear automatically within the new E-mail.

Alarm definition setup

- 1 Open the **All workstation** window. Click in the **E-Mail Recipient** radio button and type in the **URL** of your recipient as shown below. The **Notes** field is optional for information regarding the recipient.



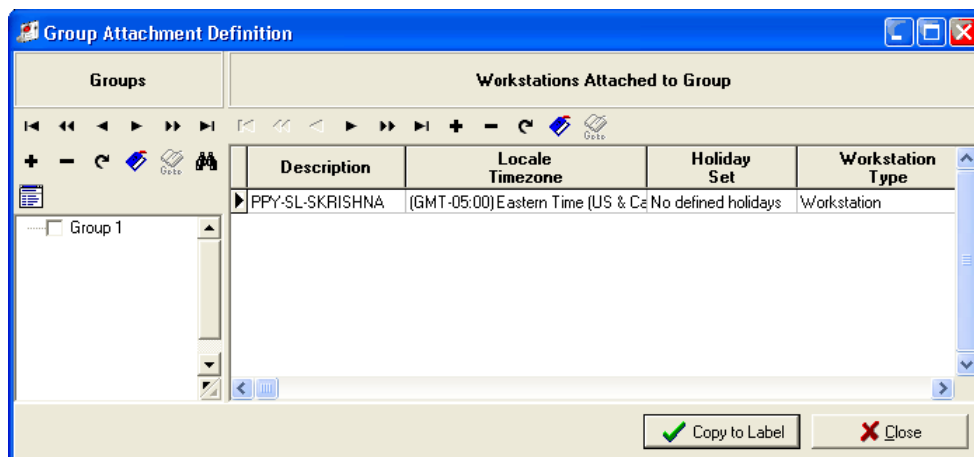
The **Workstation Definition** dialog box has a menu bar with **File**, **Search**, and **Help**. It contains two radio buttons: **User Alarm Workstation** and **E-Mail Recipient** (which is selected). Below the radio buttons is a text field containing `name@company.com`. Underneath is a large text area labeled **Notes**. At the bottom, there are two fields: *** Holiday Set** with the value `No defined holidays` and *** Locale Timezone** with the value `(GMT-05:00) Eastern Time (US & Canada)`. The dialog box has three buttons at the bottom: **Save and Close**, **Save and New**, and **Close**.

- 2 The **Holiday Set** and **Locale Time zone** fields are to be associated with the physical location of the recipient. This is most important in large networks that may include different countries and time zones.
- 3 Complete the remaining screen selections and save your changes once again.
- 4 The method used to copy workstations to groups is the same for **Operators and E-Mail Recipients**.

Attaching Groups with Labels

Once all the Group/Workstation associations are made, the Groups must then be attached to Labels.

- 1 Select the **Groups** that are to be associated with a specific Alarm Label. Verify that the Alarm Label also has a check mark in the **Selected** field then click **Copy to Label**.



The **Group Attachment Definition** dialog box has a menu bar with **File**, **Search**, and **Help**. It is divided into two main sections: **Groups** on the left and **Workstations Attached to Group** on the right. The **Groups** section has a list box containing `Group 1`. The **Workstations Attached to Group** section has a table with the following columns: **Description**, **Locale Timezone**, **Holiday Set**, and **Workstation Type**. The table contains one row with the following values: `PPY-SL-SKRISHNA`, `(GMT-05:00) Eastern Time (US & Canada)`, `No defined holidays`, and `Workstation`. At the bottom of the dialog box, there are two buttons: **Copy to Label** (with a green checkmark icon) and **Close** (with a red X icon).

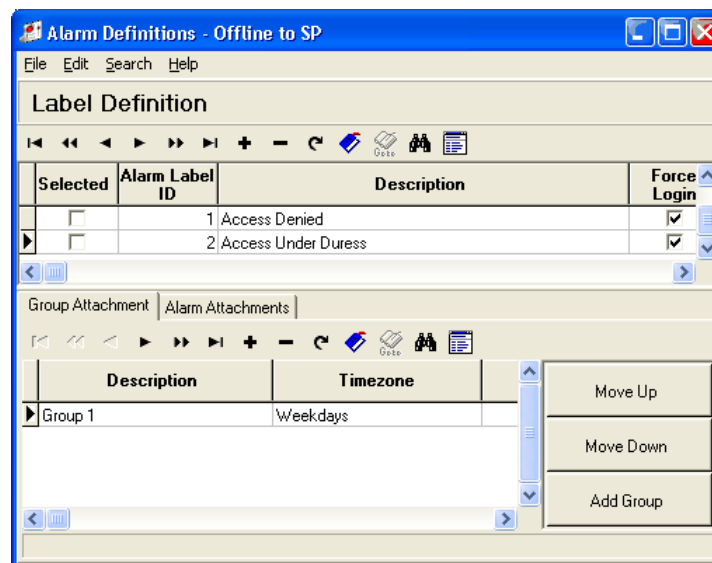
- 2 A confirmation window will appear. Click **Yes** to continue the copy or **No** to go back and make changes.

- 3 When you click **Yes** to continue, a **Group Attachment Dialog** opens. Here you need to assign a Time zone, Alarm Priority and Acknowledge Time that is specific to the group you have just confirmed. You will be prompted to select a label to copy to if you have not done so.

- a) **Time zone** - Click the expand button to open the Select a Time zone screen, highlight your choice and click OK. Use the View Time zone Interval Chart button to review the exact settings for a particular Time zone. This selection determines when you wish this group to receive this particular Alarm. Again, the physical location of the Group is the main consideration. You can define custom Time zones in System Manager to suit your Alarm routing setup.
- b) **Alarm Priority** - Defaulted to 1 (one), this setting determines the order of appearance on the Alarm Monitor display screen. The higher the number, the lower the order of importance, hence display order.

Note: As each Group is attached to an Alarm Label, you should determine at that time what the importance, or Priority, of the Alarm Label should be for each Group.

- c) **Acknowledge Time** - This number sets how many minutes an alarm will remain on display at one workstation before being routed to the next in the sequence. The sequence or routing order of Alarms is set in the Main screen. The order in which the Groups appear here will be the routing order of the Alarm. Highlight the Group record and click the Move Up or Move Down buttons to arrange the routing order of your Groups.



Alarm Attachments

- 1 To attach an alarm to a group, click on the **Alarm Attachments** tab and then on the + icon on that tool bar to open the **Alarm Attachment Definition** window.

- 2 As shown in the previous illustration, enter the Description of the alarm and notes about it. You need to select the rest of the items in the window as they apply:
 - a) **Time zone** - Click the expand button to open Select a Time zone window. This field refers to how often you wish to monitor this type of transaction.
 - b) **Transaction Group** - Click the expand button to open Select a Transaction Group window. The selections made for Transaction Groups determine the device types available in the Devices in Attachment selection.
 - c) **Transactions** - Click the expand button to open **Select Transactions** window.
 - d) **Cardholders in Attachment** - If the Transaction Group selected involves Cardholders, click the expand button to add Cardholders. (If the Transaction Group does not require Cardholders to be attached, an information message will be displayed to report this. At this point you will be prompted to save changes before continuing. Click **Yes** and the Cardholders in Alarm window opens and you may choose Add Cardholders or **Add All Cardholders**.

The Add Cardholders button will activate the Cardholder Search feature for you to make your selections.

- 3 Make your selections (you can multi-select records), click **OK** or click **Close** to return to the Alarm Attachment Definition window.
- 4 If you choose the All Cardholders button a confirmation message is displayed. Choose **Yes** to continue.
- 5 **Devices in Attachment** - Click to open the Devices in Alarm window where you can view devices already selected and Add devices. By clicking on the Add Devices button, the Reader Selection window is displayed. Three tabs will display: Controller Tree, Area Tree and a tab for devices (this is the default tab). Select the devices that will be used to trigger your Alarm. As with the Add All Cardholders option, Add All Devices functions the same way and will also display the warning message before executing the command.

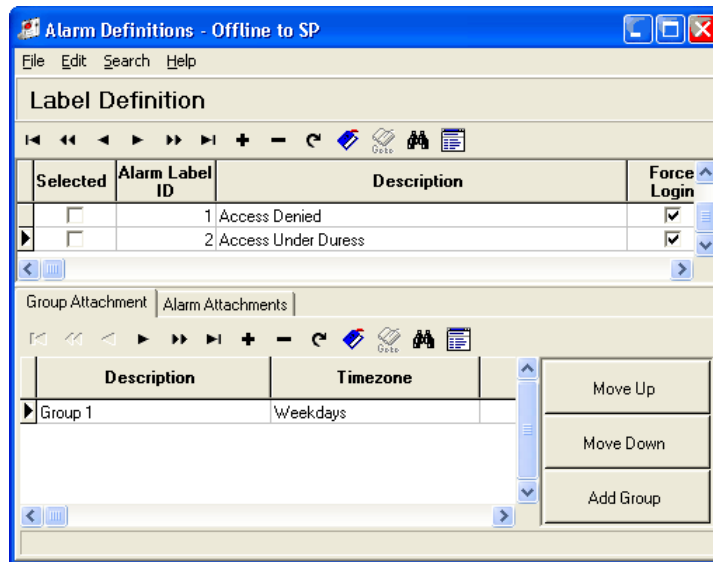
Note: The transactions selected earlier will determine what devices appear in this window.

- 6 After all selections have been made and you return to the Main Alarm Definition window, the new Alarm Attachment is listed. You may click on the (edit record) button or double click on the text in any of the fields for the record you choose in order to view or edit the details for that record.

Note: The **Search** features can be used in the same way as described in the Alarm Definition section.

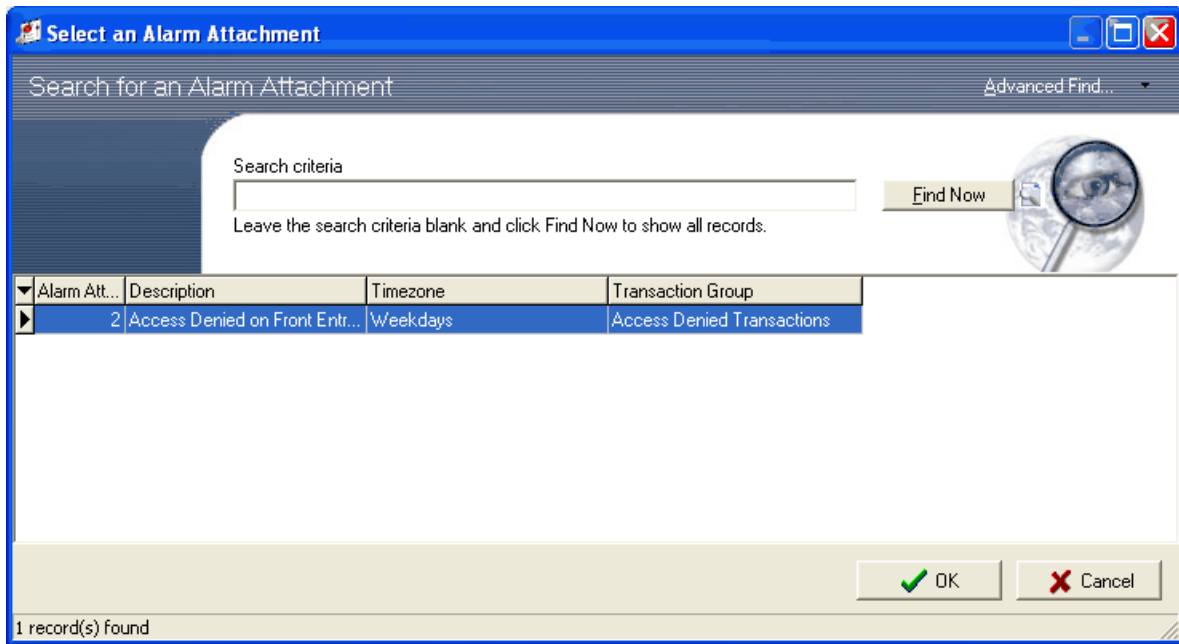
Viewing the main screen

Now that you have defined your **Groups**, **Workstations** and **Alarms** you will be able to view and edit their fields from the main screen.



Search

Find Alarm Attachments by Device - This option is mainly used for troubleshooting purposes; this opens a search window of the same name used to locate alarm attachments for a previously identified device. A tree is displayed that starts off with the Device Type in the root, then Device, Alarm Labels and Alarm Attachments. You can filter down the tree list by typing in a device id or device description and hitting the search button. When you double click an alarm label or alarm attachment, it will locate the record in the appropriate grid in the main form.



- 1 Open the generic search dialog by clicking on the binoculars.
- 2 Enter the search word in the search criteria field and click on **Find Now**.
- 3 The search result shows all the records corresponding to the search entry.

Note: When you enter a word to search for, the system puts a wild card after the search entry and search returns all the fields with the search criteria.

Advanced Find

Using Advance Find, you can build the search criteria by selecting appropriate entries from the drop down list box and entering specific value in the value field. You have to select a specific field name, condition and a specific search value.

Advance Find feature uses Boolean logic to create complex and highly precise searches. Boolean logic uses three connecting operators (NOT, AND OR) to narrow or broaden a search or exclude a term from the search. It is the process of linking criteria to narrow or expand a search through the use of **NOT, AND** or **OR**.

The Advance Find feature helps the operator to customize the search function. The operator can define the searches and save them for later use. The saved search criterion is displayed only for the operator who defined it.

- 1 Click on the **Advance Find** button to open the **Advance Find window**.

- 2 Define the criteria you want to use.



- 3 If you want to search for alarm label ID=10, you need first select left parenthesis from the list box.
- 4 Parenthesis can be used to create nested search clauses. Using the Parenthesis one can override the standard order of priority (left to right) for each Boolean statement in the search.
- 5 Select **Alarm Label ID** as the Field Name.
- 6 Select equal to (=) as the condition.
- 7 Enter the value as 10.
- 8 Provide the closing parenthesis at the end.
- 9 If you would like to specify additional search condition you can select **AND/OR** from the list box.
- 10 If you enable the NOT check box the search result will display all the records except the ones mentioned in the NOT search criteria.

E.g. if you want to search alarm IDs between 10 and 20 and between 25 and 30 you can define the search criteria as follows. Use the double parenthesis to nest a search clause.

((Alarm ID>10) AND (Alarm ID<20))

OR ((Alarm ID>25) AND (Alarm ID<30))

When you run the search you will get records corresponding to alarm ID values 11 to 19 and 26 to 29.

- 11 When you are satisfied with the criterion, click **Add to List** button. If the criterion is not valid, it is displayed in red under the Where Clause section. When the criteria becomes valid the font color changes to black.
- 12 Once you have defined the criteria click **File>Save**.
- 13 Add a description to your search and click **OK**.
- 14 The new search will be saved and listed under the **Advanced Find** button.

Editing

- 1 From the **Edit** menu select **Group Attachments**. This option opens the window to allow for add, delete and modification of group attachment records and workstations.
- 2 From the **Edit** menu select **Workstations**. This option opens the all workstations window to add and delete alarm operators or e-mail recipients, as well as for modification of existing records.

Exiting Alarm Definitions

- 1 Select **File>Exit** command to close the program.

Tool bar

The tool bar helps the user to perform the actions quickly and easily. The different arrows allow you to move between the records. The plus icon helps you to add a record and the minus icon allows you to delete a record. There is a refresh button that updates the program window. The bookmark icon helps you to mark a particular record for a later use. The *go to* icon allows you to go back to a bookmark quickly. Clicking on the binocular opens the search wizard. The edit icon allows you to edit a record at any time. Clicking on the delete icon deletes all area access privileges.



Options

Refresh SP Alarm Definitions Only When Closed

From the **File** menu select the option **Refresh SP Alarm Definitions Only When Closed**. This command sends new alarm definitions to the SP immediately for updating without closing the module.

Notes on associated Transaction Sets

The following sets of associated transactions differ from others by the manner in which they are displayed, acknowledged and secured.

- 1 **Alarmed Transactions** - These transactions generally represent the “abnormal” state of a device. They will trigger an alarm that will display to the Alarm Monitor. These alarms may be acknowledged, but will reside in the ‘Acknowledged but Not Secured’ frame of the Alarm Monitor screen. In other words, they can’t be Secured until the device itself has been restored to “normal”.
 - **Contact Active**
 - **Lost Link to Reader**
 - **Lost AC Power to RC**
 - **Battery Power Low at RC**
 - **Communications Lost to Slave Controller**
 - **CIM Lost Link to RC**
- 2 **Non-Alarmed Transactions** - These are indicative of the device’s return to its defined “normal” state. When these transactions or conditions occur, the associated pending alarms in ‘Acknowledged but Not Secured’ will simply drop from the Alarm Monitor screen.
 - **Contact Secure**
 - **Restored Link to Reader**

- Restored AC Power to RC
- Battery Power Normal at RC
- Communications Restored to Slave Controller
- CIM Restored Link to RC

Door Forced Open/Door Held Open Alarms

Old Method

The concept of Door Forced Open was introduced with the release of software version 5.0.7. This initial concept was tied to the relay type called "GO", which controlled the door strike. The system uses the following two terms to define the state of the door.

- DOD secure
- DOD active

If the door experiences a transition from closed (DOD active) while the GO relay is de-energized (released), the door was forced open.

The screenshot shows the 'Contact Definition' dialog box with the following fields and settings:

- Description:** Contact1
- Notes:** (Empty text area)
- * Attached to Which Controller or Reader:** Template3 - DOD is being Self Shunte
- * Location:** (Empty field)
- * Contact Type:** DOD
- * Associated Elevator Reader:** (Empty field)
- Alarm Samples:** 2
- Fault Samples:** 16
- Parallel Resistor:** 0
- Series Resistor:** 0
- Debounce Period (Seconds):** 0
- Input Number:** 1
- Verify Status:** ☐
- Normally Open:** ☒
- Installed:** ☒

At the bottom, there are three buttons: 'Save and Close', 'Save and New', and 'Close'.

For implementing this functionality, the DOD contact should be downloaded to the controller based on the contact device. To define this, a contact type (DOD) should be specified in the contact definition field.

The GO relay definition also should be downloaded to the controller. This can be defined on the **Relay Definition** screen by specifying a relay type called "GO".

The screenshot shows the 'Relay Definition' window. The title bar is blue with a red close button. The menu bar includes 'File', 'Edit', 'Search', and 'Help'. The main content area has the following fields:

- * Description: Relay 1
- Notes: (empty text area)
- * Attached to Which Controller or Reader: Template1 - Card Reader for Entry (No REX) (No DOD)
- * Location: Development Room
- * Relay Type: GO
- * Associated Elevator Reader: (empty)
- Relay Number: 1
- ☒ Installed

At the bottom, there are three buttons: 'Save and Close', 'Save and New', and 'Close'.

To implement this concept, the SRCNX required knowledge regarding the state of the GO relay. The reader interface firmware was modified to report the status of the GO relay. The 5.0.7 version of the Door Forced Open required the following versions of firmware and software.

RINX Firmware	HC11 Firmware	RCNX Firmware	RCNX2 Firmware	Software
RINX03	HC11W6	5.60	5.45	V5.0.7

New Method

The concept of Door Forced Open was modified to the following:

Report Door Forced Open any time the door (DOD) contact goes from secure to Active with no shunt applied.

If the door was expected to open, a shunt would be applied to the DOD contact and no transaction would be generated. A Request to Exit (REX) mechanism must be defined to generate the DFO transaction. If the door has no request to exit (REX) mechanism, then the Door Forced Open feature should be disabled. Installing a self-shunt on the Door Open Detect (DOD) contact enables the door forced open feature. This is accomplished by setting up an action on the DOD contact to shunt the DOD contact for a period of time. The triggers are executed before transactions are reported. When transactions are reported, contact is shunted from reporting and the transactions are ignored. When the timer expires, if the DOD contact is still active, the system reports Door Held Open.

This concept eliminated the need for the relay status to make the Door Forced Open decision. Since the relay status is no longer required, we eliminated the need for any custom reader interface firmware.

A transaction called “Door Held Open” was introduced with version 5.0.8, which will be generated whenever the DOD shunt timer expires and the door remains open. This will help identify a class of alarms, which can easily be defined in an alarm group.

The version requirements became:

SRINX Firmware	HC11 Firmware	SRCNX Firmware	SRCNX2 Firmware	Software
Any	Any	5.62	5.62 w/o DHO	V5.0.8

The following table explains the exact performance of Door Forced Open functionality for various combinations of firmware and software available in the fields.

SRINX		SRCNX	SRCNX 2	Software	DFO	DHO
Any		<5.60	<5.45	Any	No	No
<HC11W6		5.60	5.45	Any	No	No
<RINX03		5.60	5.45	Any	No	No
HC11W6 or RINX03		5.60	5.45	<v5.0.7	Error	No
HC11W6 or RINX03		5.60	5.45	V5.0.7	Yes	No
HC11W6 or RINX03		5.60	5.45	V5.0.8+	Yes	No
Any		5.62		<v5.0.7	Error	Error
Any		5.62		V5.0.7	Yes	Error
Any		5.62		V5.0.8+	Yes	Yes

SRINX	SRCNX	SRCNX 2	Software	DFO	DHO
Any	5.63	5.62	<v5.0.7	Error	No
Any	5.63	5.62	5.0.7	Yes	No
Any	5.63	5.62	5.0.8	Yes	No
Any	5.63	5.62	5.0.9+	Yes	Yes

Implications

The following tasks must be performed in the firmware to support Door Forced Open functionality.

- 1 Any triggers on DOD contacts for Contact Active transactions should be evaluated and changed to trigger on the Door Forced Open transaction or the Door Held Open transaction. Depending on the actions taken with DHO and DFO transactions, triggers will have to be modified to recognize the differences between contact active, door forced open, and door held open.
- 2 The Door Open Detect trigger behaves as:
- 3 When the Door Forced Open transaction is reported, DOD Contact Active trigger is executed followed by DOD Door Forced Open trigger.
- 4 When the Door Held Open transaction is reported, DOD Contact Active trigger is executed followed by DOD Door Held Open trigger.
- 5 Any alarms on DOD contacts for Contact Active will have to be changed to alarm on either Door Forced Open or Door Held Open. In some cases, another alarm will have to be defined to recognize the difference between Door Held Open and Door Forced Open.
- 6 If there are contacts defined as DOD contacts, which do not perform the Door Open Detect function, then these contacts will have to be modified to a contact type, which more accurately defines the function of the contact. If these contacts are not changed they will begin reporting Door Forced Open instead of Contact Active and the associated alarms and triggers will fail.
- 7 The illustrations in this chapter have included Contact Alarms. The steps for defining all alarms are basically the same. The difference with these two types of alarm is that the programming of your devices must also be specific, and there are software and firmware requirements as well.

Note: This feature requires SRINX firmware revision 03 or higher or HC11 firmware version W6 or higher.

Programming for SRINX or HC11- Under your Contact Alarms label, in the Alarm Attachments tab, create an attachment for Door Forced Open/Door Held Open. The Transaction Group is Contact Transactions and you must select both the Door Held Open and Door Forced Open transactions. This is done so the system will differentiate between a door held open beyond the defined shunt time for a valid entry or access and a door that is actually forced open; then send the appropriate alarm.

With SRCNX-2 - The Alarm programming is the same. Hardware devices are defined differently in System Manager with this board and triggers must have the correct device associations.

- Reader Trigger Associations
- Reader 1 = Go Relay 3, Contact 1 Rex, Contact 2 DOD
- Reader 2 = Go Relay 4, Contact 3 Rex, Contact 4 DOD

Reference sections:

System Manager/Hardware Map and sub-chapter Event Triggers explain how to define devices and triggers.

Alarm Monitor

CHAPTER 17

Introduction

The **Alarm Monitor** gives you flexible and programmable monitoring of virtually any alarm condition. It is a program that helps you to view, acknowledge and secure all alarms that you have defined in your system. There are two types of alarm monitors. The first is a Workstation Alarm Monitor, which displays alarms that are programmed to appear on predefined workstations. The second is an Operator Alarm Monitor, which displays alarms wherever selected operators are logged into the system. An E-mail Recipient can be defined as well to receive messages upon specific alarms. Procedures for defining the Alarm Monitors are covered in the preceding Alarm Definition chapter.

Alarm information

When an alarm is triggered, the system sounds an alert and displays the Alarm Monitor screen at a designated Workstation or at the location(s) where Alarm Operators are logged on.

The highest priority alarms will be at the top of the screen, indicating they require immediate attention. A User ID and password, comments or other actions may be required in order to acknowledge an alarm, depending on how it was programmed. E-mail Recipients can be created and receive instant notification when critical alarms are triggered.

If the alarm has a **Sound File** attached, when the alarm occurs, the system plays the recorded sound file. The sound file can be attached with the alarm, when the alarm is defined in the Alarm Definitions program.

Working with Alarm Monitor

Starting the Alarm Monitor

Note: The Alarm Monitor icon does not appear in the System Launcher.

This module must be added to the **Start up** tab in **System Security** for each workstation that is to receive alarms. To do this, go to **System Security\Startup**, click **Add** and select Alarm Monitor.

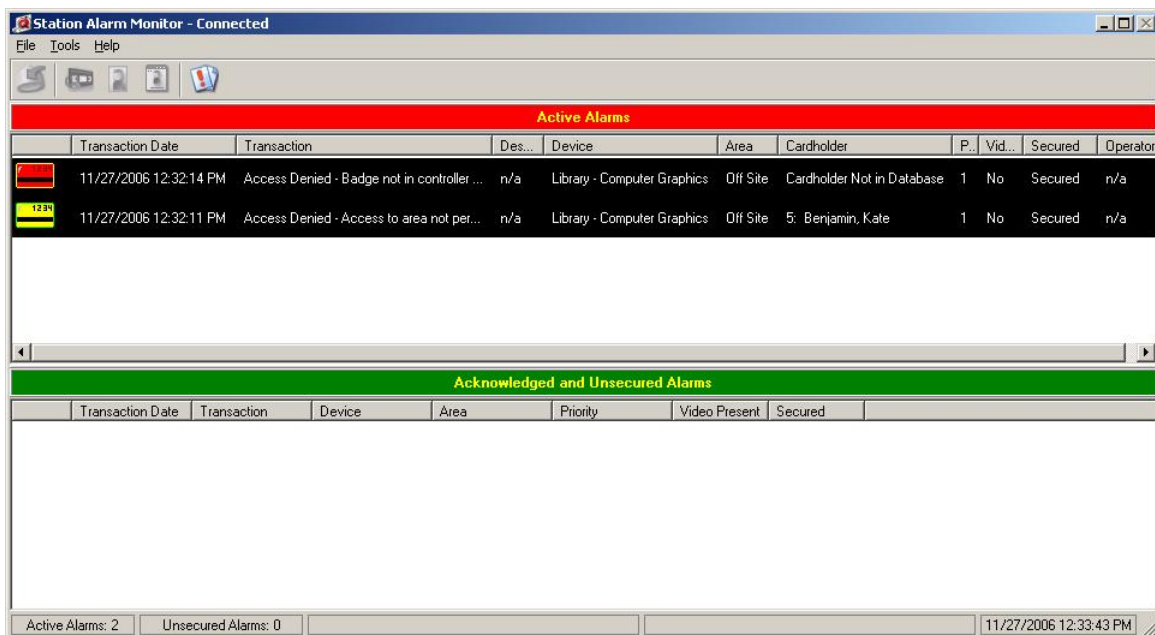
Note: If a Workstation is not attached as part of a routing group, Alarm Monitor cannot be enabled.

If an alarm operator logs into a computer that is *not* defined as an alarm workstation, or where the **Alarm Monitor** is not placed in the **Start-up** tab, the Alarm Monitor still opens as long as the alarm operator is defined as part of a routing group.

When the alarms appear, only users with the proper rights will be able to acknowledge. Remember to give the proper Alarm Monitor Privileges (at least *Read-Only* rights) to the users that are defined as Alarm Monitors or they will not be able to respond to the alarms.

Active Alarms

This section displays incoming alarms and those are not acknowledged. The color schemes for the alarm display are customized in the **Alarm Definition** module.



Acknowledged and not secured

Certain alarm transaction types relate to the normal physical state of a device. When the normal state of the device changes, an alarm is triggered. While the alarm may be acknowledged, it will display in this section until the device has physically been returned to the normal state. The example below shows a Controller Alarm for a CIM Lost Link to RC. This alarm will remain here until the connection to the controller has been restored. The transactions or conditions that will secure these types of alarm are Contact Secure, Restored Link to Reader, Restored AC Power to RC, Battery Power Normal at RC, Communications Restored to Slave Controller and CIM Restored Link to RC.

Pre-defined Alarm Comments

Schlage SMS provides a program for the Administrator to set pre-defined comments for the operator to enter while acknowledging the alarms. Follow these steps to define alarm comments.

- 1 Open the **Pre-defined Alarm Comments** program from the System Launcher. To add new set of comments, click on the plus sign in the **Pre-defined Comments** window.
- 2 Enter the comments in the **Pre-defined Comments Definition** window.
- 3 Click **Save and Close** to save the application and return to the main window. Click **Save and New** to save the current definition and define a new one. Click **Close** to close the Definition window without saving the defined comments.

While defining alarms, the administrator can attach these comments with the alarm. The operator shall be able access these comments from the **Alarm Details** window while acknowledging the alarms.

Acknowledging Alarms

When an alarm occurs, the system alerts the operator by displaying the Alarm Monitor on the screen. The alarm remains on the screen until the operator acknowledges it.

As a part of establishing standards for alarm acknowledgement, the administrator can set parameters that force the operator to enter comments either free-form or by selecting pre-defined comments. The parameters can be set while defining alarms in the Alarm Definition program.

Follow these steps to acknowledge an alarm.

- 1 Select the alarm that you want to acknowledge from the Alarm Monitor screen. Right click on the alarm and select the option **View Alarm Details** from the menu.
- 2 You can also access the **Alarm Details** (see "Acknowledging Alarms" on page 284) window by selecting **View Alarm Details** option from the **File** menu or double clicking on a selected alarm.

- 3 The **Alarm Details and Comments** window is displayed.

Alarm Details and Comments

Alarm Priority: 1

Alarm Date and Time: 5/15/2007 1:57:06 PM

Alarm Transaction: Access Denied - Badge not in controller memory

Secured: 5/15/2007 1:57:06 PM

Acknowledged: Unacknowledged

Acknowledged By:

Controller: Main board

Device: Rdr on Ch 3

Cardholder: 330: Anderson, Tom S

Operator: n/a

Description: n/a

Live / Recorded Video | Alarm Instructions | **Alarm Comments** | Cardholder Images | Overrides

Alarm Comments

Called security.

Comment	Operator	Date and Time
Called security.	Administrator, System	5/15/2007 1:57:44 PM

Insert Comment | Insert Predefined Comment

Acknowledge Alarm | Close

Alarm 1 of 1 | Current User: USR

The left hand side of the Alarm Details window displays the following information.

- Alarm Priority** - This indicates the level of priority of the alarm.
 - Alarm Date & Time** - The date and time the alarm has occurred is displayed in this field.
 - Alarm Transaction** - The transaction that caused the Alarm.
 - Secured** - Whether the device that is attached to the particular alarm is secured or not.
 - Acknowledged** - Whether the alarm is acknowledged or not.
 - Acknowledged by** - The name of the Operator who acknowledged the alarm.
 - Controller** - The controller that is connected to the device which generated the alarm.
 - Device** - The device that generated the alarm. (E.g. In a situation where there is an alarm called "Lost Link to Reader", the Reader is the Device. The name of the Reader will be displayed in this field.)
 - Cardholder** - If the alarm is a cardholder alarm, the name of the cardholder is displayed here.
 - Operator** - If it is an operator alarm (E.g. illegal login) the name of the Operator is displayed in this field.
- 4 The right hand side of the window contains instructions to the Operator and the comments that are entered by the operator.
- 5 Click on the **Alarm Instructions** button to see the instructions to the Operator. These instructions are entered in the **Alarm Definition** (on page 264) program, when an alarm is defined. The administrator can attach a .wav file with each instruction.

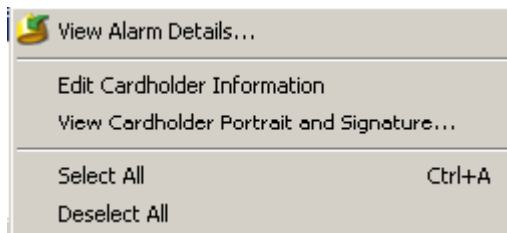
- 6 Depending on how the alarm was defined, you may be required to provide User ID or comments for the highlighted alarm before the system accepts the acknowledgment command. The administrator can *"force login"* and *"force comments"* before letting an operator to acknowledging an alarm. If this is the case, the applicable window opens for you to enter said requirements and acknowledgment will be accepted.
- 7 While entering comments you have the option to select the pre-defined comments or enter comments free-form.
- 8 Click on the **Live/Recorded Video** (see "Receiving video of alarms" on page 288) tab to view the video associated with the alarm.

Note: The Live/Recorded Video option is available only for cardholder and contact transactions. You also need to have **SEVMS** server installed in order to receive video of alarms. Transactions can be attached to cameras using the **SVTR Camera Definition** (see "SVTR" on page 474) module.

Viewing and editing Cardholder information

Alarm Monitor also allows you view the portrait and signature of the cardholder (provided you are viewing a card alarm) in question to reassure the security further.

- 1 Right click on the Alarm and choose **View Cardholder Images** option from the menu.



or click on the tool bar icon shown below.

View the portrait and signature of the selected Alarm



- 2 The cardholder portrait and signature are displayed.



- 3 The user can choose to view either portrait or signature only or clear both. Click on the **View** menu and select the appropriate option.
- 4 If you want to snap the Portrait window to the corner of the screen, click on the **Tools>Options**. In the settings window specify the number of pixels at which you want to snap the window to the right or left corners.
- 5 You can also view or edit the information about the cardholder in question. You can access the **Cardholder Definition** program from the Alarm Monitor screen itself, and edit the information. This feature helps the Operator to give or deny access to a particular cardholder. To perform this functionality, the Operator *must have* Read/Write privilege to the Cardholder Definition application. Right click on the transaction and select **Edit Cardholder** in **Cardholder Definitions** Program.

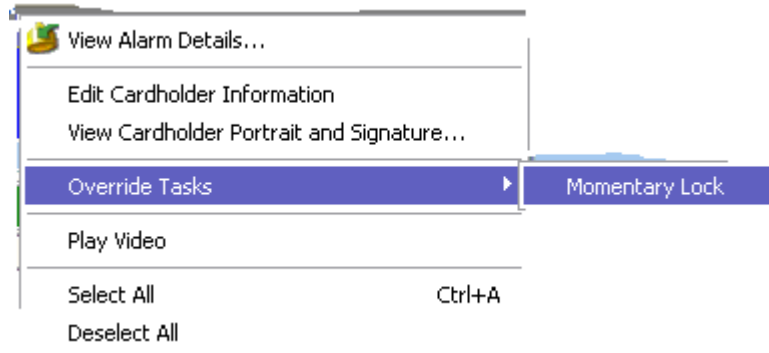
Viewing Previous Alarms

If you want to view alarms that occurred previously, click on the **View Previous Alarms** from the **File** menu. It opens the program for running reports on alarm history. Details for this module are found in the Report Launcher chapter.

Executing Override Tasks

When an alarm occurs, the operator can execute necessary actions using the Override Tasks that are defined in the system. The system shows all override sets and tasks that have the alarmed device as an associated device for the override tasks or the device that the action affects for an override action.

To execute these Override Tasks, right click on a alarm and select **Override Tasks** from the menu, and click on the override you want to execute.



Receiving video of alarms

If there is Schlage Enterprise Video Management System (**SEVMS**) attached to your **Schlage SMS**, you can receive video of certain transactions that occur in the system. The cameras and video servers are defined and attached to alarms using the **SVTR Camera Definition** (see "SVTR" on page 474) module. You can receive video of only cardholder (Access Denied and Access Granted) and contact transactions. The Alarm Monitor and Alarm Graphics programs are capable of displaying live and recorded video. The recorded video can also be displayed in a separate window so that the user can still view the live video while viewing the recorded video.

- 1 You can play the video by clicking on the **Play Video** icon on the main window of Alarm Graphics, Alarm Monitor and Transaction Monitor.

- 2 The video of the transaction from the camera is displayed on your monitor screen. This helps you to get potential information of all the alarms. You can perform the playback functionality using various buttons appear on the screen.



To receive video of transactions in the Alarm Monitor/Alarm Graphics, the user has to define the transactions, device that generates the transaction and the camera that is associated with it in the **SVTR** (on page 474) module.

The user also has to define transactions as alarms in the **Alarm Definitions** (see "Alarm Definition" on page 264) program to receive alarms.

You can also receive live video on the Alarm Monitor/Alarm Graphics while viewing the recorded video of a transaction. In the **Alarm Details** (see "Acknowledging Alarms" on page 284) window click on the button **Live Video/Recorded Video** button. The video from the camera associated with the transaction (alarm) is displayed on the screen. The order different tabs you see on the Alarm Details and Comments window can be changed by dragging the selected tab and dropping it in the desired location.



The left pane displays the live video and the right pane displays the recorded video of the transaction. The windows and tabs can be resized and the system saves the changes per user. The **PTZ** (Pan, Tilt, Zoom) **Control** allows you to view the different angles of the camera in the live video section. In the recorded video section, various buttons are available to play the video, stop the video, play the next frame, play the previous frame, begin the video and end the video. Move the mouse over these buttons to see the captions for each button.

Note: If the camera does not have PTZ capability, the PTZ Control is not displayed along with the live video. For more information about the controls available on PTZ Control panel, refer to the **SEVMS** manual.

Sorting tabs

Users can rearrange the order of the tabs on the Alarm Details and Comments window using the drag/drop feature. Click on a tab and drag it to the desired location.

PTZ Panel

The PTZ Panel is used for cameras that support the Pan, Tilt, and Zoom functionality. If the associated camera is a PTZ camera, this panel is available through the modules that show live/recorded video of transactions (Alarm Monitor, Alarm Graphics and Portrait Monitor).

The following are the different functions available on this panel. The green signal indicates that the PTZ control is connected.

Change the camera angle - Changing the camera angle is done using the different arrows that are shown on the panel. This can be also done using the <Home>, <PgUp>, <End> and <PgDn> buttons on the right side of the keyboard.

Focus - Use the up and down arrows to adjust the focus of the camera.

IRIS - Iris buttons allow for light adjustment of the camera. Iris is an adjustable diaphragm of thin opaque plates that can be adjusted by the + and - buttons so as to change the diameter of a central opening usually to regulate the aperture of a lens.

Zoom - You can enlarge or decrease the size of the image by clicking on the up and down arrow buttons.

Speed - Using the sliding bar, you can adjust the camera movement.

Moving the camera to a preset Location - To go to a pre-set camera location use the **Send** button, it opens the extended panel. Enter the number of the camera location and click **Enter**.

Setting a new location - To set a new location move the camera to the desired location and click on the **Set** button. It opens the extended panel. Enter a camera location number and click **Set**.

Note: This feature is not activated in the PTZ Panel available through **Schlage SMS** modules. In **Schlage SMS**, the camera positions are pre-set using the **SVTR Camera Control** (see "Working with SVTR Camera Control" on page 474) module.

Aux On - To run a pre-set Auxiliary tour use the **Aux** button. The green signal shows the PTZ control is connected.

Step - There are modes in which a PTZ camera can be operated. Using the continuous mode allows a smooth and continuous movement of the camera when using the moving panel or the arrows as explained above. Pressing either on the middle button in the moving panel, on the space bar, or on "5" on the right hand side of the keyboard stops the camera movement. The step mode brings about a non-continuous movement. Each step allows the camera to move 1000 milliseconds. In the image above the number of steps is two, therefore the camera moves to the requested direction a period of 2000 milliseconds, then it stops.

Extended Control

Note: Based on the camera specification the extended control is enabled. Example a Pelco Spectra III series camera supports the extended control.

The **Auto Pan Stop/Start** button is used to pan the camera continuously until it is stopped. The Set pattern and Pattern start buttons are used to program and pan set patterns.

Printing the Alarm screen

To print the current display of Alarm Monitor, click on the *Print Alarm Screen* button from the **File** menu.

Minimize Alarm Monitor

Clicking on the **Minimize the Alarm Monitor** option from the **File** menu will minimize the screen to the task bar; if alarms exist that have not been acknowledged, the screen will continue to pop up until they are attended.

The Close command is not available on the Alarm Monitor screen. The module cannot be closed down on an Alarm Workstation without exiting the Launcher and Schlage SMS completely. An Alarm Operator must log off to close the Monitor. If you want to snap the alarm monitor window to the right or left corners of the screen, click on the **Tools** menu and click *Options*. In the **Settings** window specify the number of pixels at which the Alarm Monitor window snaps to the corner of the screen.

Previous Alarms

CHAPTER 18

Introduction

The View Previous Alarms module gives an accounting of alarms that have occurred and the comments attached with it. You have the ability to select the type of alarm, the date and time range of activity, running a specific report to the screen and printing it out.

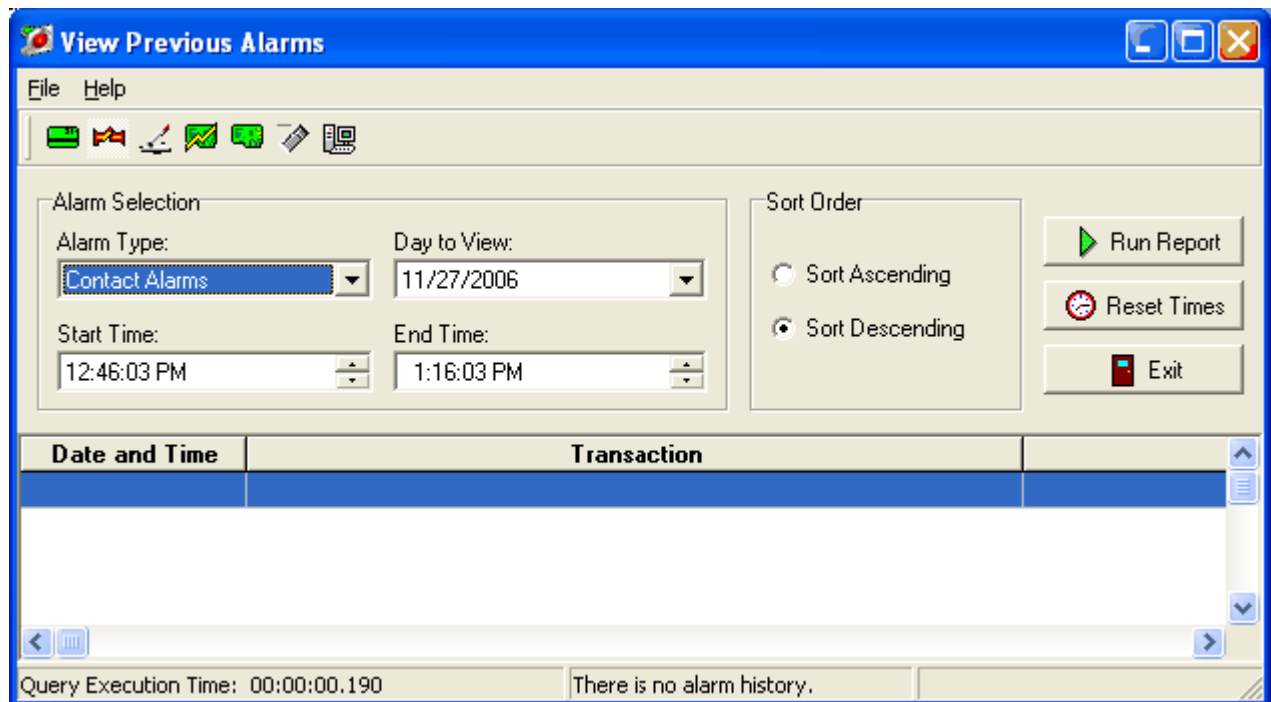
Accessing the application

- 1 Open the **Schlage SMS** by double clicking the **Schlage SMS** icon on your desktop choose Start>Programs>Schlage SMS>Schlage SMS.
- 2 The login window, opens. Enter your user ID and password.
- 3 In the System Launcher window, double click on Previous Alarms icon.

Note: You can also open the View Previous Alarms module through the **Alarm Monitor**.

Working with Previous Alarms

The main screen consists of the menu and tool bars, alarm selection, sort order and report controls, display grid, and the status Bar. Details follow for all screen features.



Running a report of Alarms

In order to run a report of alarms that occurred in the system you need to first specify the alarm type, date and start and end time.

- 1 First select the alarm type. The down arrow will open the Alarm type selection menu. The different alarm types available to choose from are Card, Contact, Relay, Communications, Controller, Operator, System, Guest, and Tour Alarms. You can only choose one alarm type at a time.
- 2 Then select the day to view. The current date is the default. Click on the down arrow to display the calendar and click on the day you wish to view. A red circle appears around today's date and the day chosen will be highlighted.
- 3 Use the up and down arrow to adjust the start and end time of the alarm reports.
- 4 Then select the sort order. You can select either **Sort Ascending** or **Sort Descending**.
- 5 Select Run Report. This will execute the query and displays the information
- 6 To reset the start and end time, click on **Reset Times**. After manually changing the start and end times and running a report, this will reset the times to your defaults.

- 7 The fields of information returned from the history database tables are shown in the **Display Grid**. This information may vary slightly depending on the type of alarm selected. The **Query Execution Time** at the left hand corner of the window is simply the time it took for the query to run and return the selected report information. At the right, the First and Last fields are the dates and times of the first and last entries in the database alarm history table.
- 8 Click **Exit** to close the application.

View Alarm Comments

When an alarm is acknowledged, the operator may enter comments at that time and are what the screen below will display. Additional comments may be added here as shown.


- 1 Select **File>View Alarm Comments**. The **Existing Commands** section displays the predefined comments for the alarm. You can also double click on an alarm to enter this window.


Options


- 1 **File>Print Screen** – sends the main screen report information displayed to the printer
- 2 **File>Display Defaults** - system default times are shown in the dialogue.


Tool bar


The tool bar icons combine the tasks of selecting the alarm type, resetting the time range to the defaults you have set, and running the report. The name of the transaction represented appears in a hint displayed when you pass the cursor over the icon (only the most commonly used transaction types have icon buttons).


Card alarms - 

Contact alarms - 

Communications alarms - 

Controller alarms - 

Operator alarms - 

System alarms - 

Alarm Types

The following are the different alarm types available.

All reports include the following items of information; only relative or additional items will be listed for each report type.

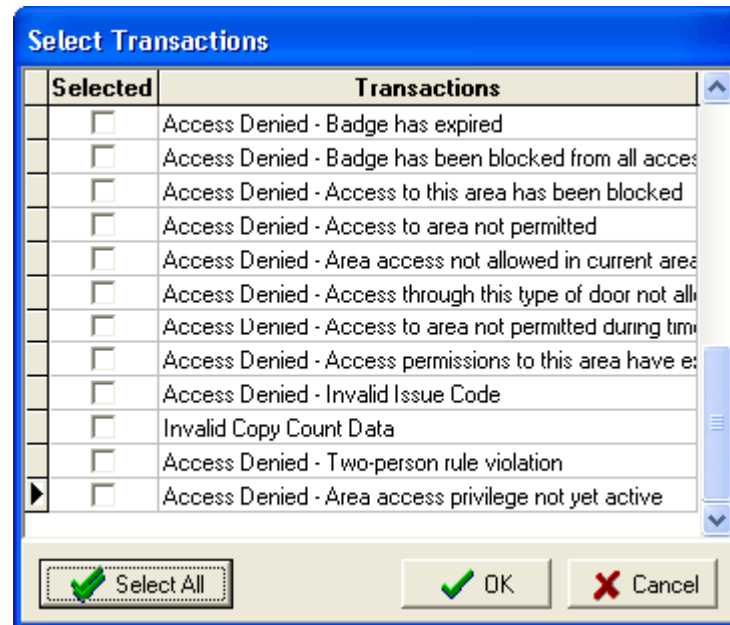
- 1 **Date and Time** – date and time of the alarm
- 2 **Transaction** – transaction that generated the alarm
- 3 **Device** – the device name that generated the alarm
- 4 **Acknowledged\Secured** - date and time alarm was acknowledged and secured, or 'not secured' if applicable
- 5 **Area** – the location of the device
- 6 **Controller** – the controller that the device is attached to.
- 7 **Acknowledged** – date and time of acknowledgment
- 8 **Acknowledged By** - user ID of the person who acknowledged the alarm
- 9 **Cardholder Name** – if applicable, cardholder's name that used the card or the status of the card (i.e. "card not in database...")
- 10 **Encoded ID** – from the cardholder badge information

Card Alarms

Alarms attached to cardholder transactions are called card alarms.

- 1 **Access Granted**
 - Valid Access
 - Valid Entry
 - Valid Exit
 - Valid Copy Machine Access
- 2 **Access Denied**

See the different access denied transactions in the screen capture below.



Contact Alarms

Alarms attached to contact transactions are called contact alarms.

- Contact Active
- Contact Secure
- Trouble Open
- Trouble Short
- Door Forced Open
- Door Held Open

Relay Alarms

Alarms attached to relay transactions are called relay alarms.

1 Relay Transactions

- Relay Energized
- Relay Released

Communication Alarms

Alarms attached to the following communications transactions are communication alarms.

1 Reader Communications

- Lost Link to Reader

- Restored Link to Reader
- Lost 900MHz link to Reader
- Restored 900MHz link to Reader

Operator Alarms

Alarms attached to operator transactions are operator alarms.

- **Workstation** - name of the workstation on which the Alarm occurred
- **Operator** - user ID of the person who was using the workstation when the alarm occurred

1 Operator Alarm Transactions

- Logged In
- Logged Out
- Online Monitor Closed
- Online Monitor Started
- System Shutdown
- Alarm Display Logged Out
- Alarm Display Logged In
- System Startup
- Illegal Login
- Auto-scheduler Started
- Auto-scheduler Shutdown
- Alarm Display Logged In
- Alarm Display Logged Out
- Auto Scheduler Started
- Auto Scheduler Shut Down

System Alarms

Alarms brought about by failures of the system process are called system alarms.

1 System Alarm Transactions

- CIM Online
- CIM Offline
- CIM Started
- CIM Failure
- CIM Shutdown
- Gather from RC
- Loading RC Failure
- Update RC Failure
- Set RC Clock

- Archiver Started
- Archiver Closed
- History Archive Failed
- History Archive Complete
- History Archive Aborted
- History Archive Started

Guest Alarms

The following guest transactions can be defined as alarms.

1 Guest Pass Transactions

- Guest Signed In
- Guest Authorized
- Guest Signed Out
- Guest Reset to Pending
- Guest Deleted

Offline Lock Transactions

The number of transactions under this section is too large to list here. Please see Transactions Codes Editor>Transactions Group>Offline Lock Transactions section to see a complete list of transaction available.

RR Transactions

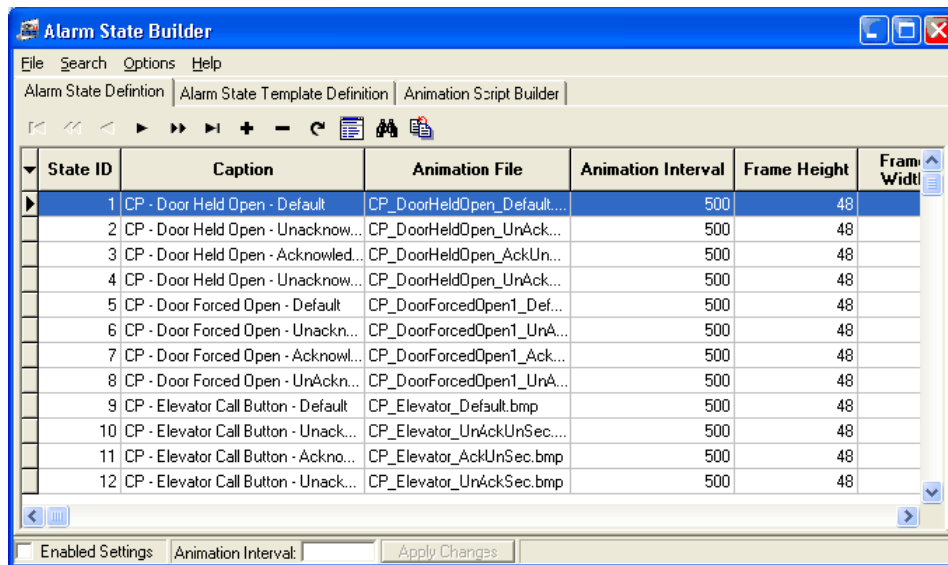
The following are the two set of transactions created by Schlage Redundant Recovery program. For a detailed view of the list of transactions, please see Transactions Codes Editor>Transactions Group section.

- 1 RR Success Transactions
- 2 RR Failure Transaction

Alarm State Builder

CHAPTER 19

The Alarm State Builder represents an easy way to associate animated graphics and icons with alarm states in the Alarm Graphics program. This program is also capable of creating custom animated graphics.



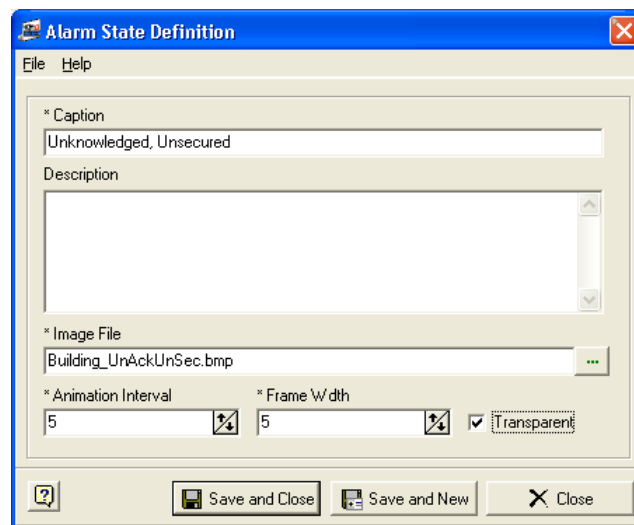
Animation Builder has three main tabs. They are;

- 1 **Alarm State Definition** - This tab is used to associate graphic files with different alarms or alarm states.
- 2 **Alarm State Template Definition** - Here you can define animation template for different alarm states. For example, if you want to define three different states of a fire alarm (unacknowledged and unsecured, acknowledged, but unsecured, unacknowledged but secured) you can create a template here.
- 3 **Animation Script Builder** - This tab helps you to create custom animated files or modify the existing ones.

Alarm State Definition

The Alarm State Builder program allows you to define a alarm state record and associate it with a particular icon or an animated graphic file.

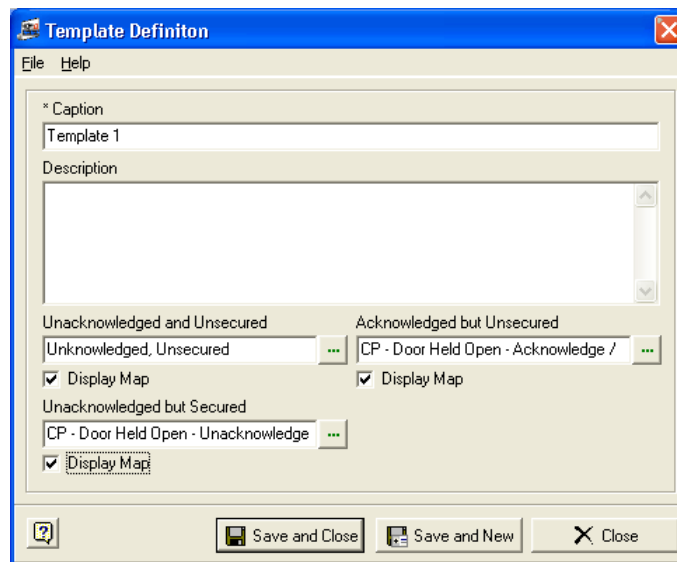
- 1 Click on the plus sign (+) sign to define a new alarm state record. The **Alarm State Definition** window is displayed.



- 2 Fill in a caption for the **Alarm State**.
- 3 Add a suitable description.
- 4 Add the pre built animation script file by clicking on the expand button. The program defaults to the C:\Program Files\Schlage\Icons folder to select the appropriate image file.
- 5 Choose an interval for your animated graphic. This interval determines how fast the image will switch between frames.
- 6 Enter a specific frame width for all your frames. Make sure that the width of the image and the frame is same.
- 7 Check the box if you want the image to be on a transparent background. If you select this option the background of the image becomes transparent and you can customize the background with different colors.
- 8 Choose **Save and Close** when you complete the Animation Definition. Click the **Save and New** button if you want to continue defining animations or icons. Click **Close** if you don't want to save the definition.

Animation Template Definition

Here the user can make a template using various kinds of graphics representing different alarm states. This template can be later used in Alarm Graphics program while defining alarms and alarm states.



Animation Script Builder

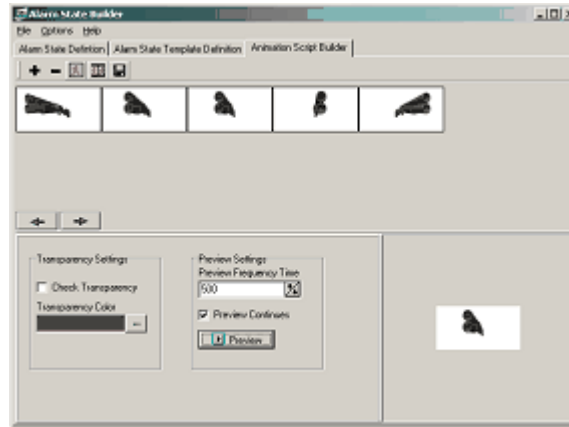
Animation Script Builder makes it easy to create and edit custom animation files. This program can also create transparent animated graphics.

You can create animated graphic by creating animation scripts. To build an animation script you need to know the number of frames that the script is going to handle and the height and width of the image. Remember that all the frames you are using for building a particular animation script must be of same height and width.

Follow these steps to build an animation script.

- 1 To build an animation script file first you need to load frames on the screen. Click on the tool bar icon "Load Frames" and the program will load frames. You can increase or decrease the number of frames that you want to use by clicking on the plus or minus signs. You can also do this by selecting **File>Load Frames**.
- 2 Once you have loaded the frames check the frame settings. The height and width of these frames should be same as the height and width of the images you are going to use. All the frames must be of same measurements to get a flawless animated file. Click on **Options>Frame Settings**. The **Frame Settings** window opens. Specify the number of frames, Frames height and Frame's width.
- 3 Now start loading images. Select **Options>Load Multiple Images**. The program defaults to C:\Program Files\Schlage\Icons folder. Select the files required for creating animation script file. If your files are in another location browse to that folder and select the files.

- 4 Once all the files are loaded correctly, you can preview the script by clicking on the **Preview** button.



- 5 Check the **Preview Continuous** to run the animation script continuously.
- 6 **The Preview Frequency Time** decides how fast you want the script to switch between frames. The lower the value the higher the speed will be.
- 7 The **left and right arrows** allow the user to change the order of the frames.
- 8 Check the **Transparency** option to make the background of the animated file transparent. Clicking on the expand button opens a color palette. Choose the color you want to use for previewing the transparency effect.
- 9 Once you are satisfied with the file you can save it by selecting **File>Save Script** or by clicking on the **Save** button.

Modifying Animation Scripts

You can also modify the existing animation scripts using this program. You cannot modify animated gif files. This program can only handle animation script files.

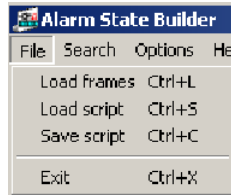
- 1 To load an animation script file, select **Options>Load Script**.
- 2 You need to select the animation script file. In the **Animation Script Window** select the animation script file and enter the number of frames used or the width of the frames. Click **OK**. The animation script is loaded on the screen.

Now you can start editing the file. You can change the order of frames, delete and replace some of the images with new images. Once you are satisfied with the changes you can save the script.

Menu options

The following section describes the features available under File, Search and Options menu.

File



File menu consists of four different options. First three options (Load Frames, Load Script, Save Script) will only be available while the **Animation Script Builder** tab is active.

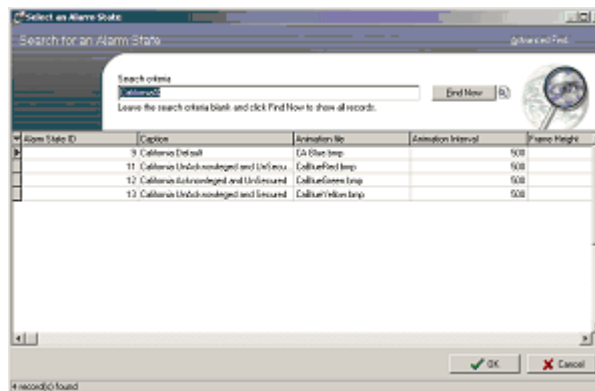
- 1 **Load Frames** - Click this option to load frames on the screen. You can add any number of frames you want by clicking on the plus sign (+) on the tool bar.
- 2 **Load Script** - This option allows the user to load an animated graphic file into the screen for editing and modification.
- 3 **Save Script** - Clicking this button saves the script you created or modified.
- 4 **Exit** - This option allows the user to exit from the program.

Search

Alarm State Builder program is equipped with a search feature, which enables the user to search and find the Alarm State Definitions and Alarm State Template Definitions easily.

To search for Alarm State Definition or Alarm State Template,

- 1 Click on the **Search** button located on the menu bar. Click **Find** option. The **Search** window is displayed. Enter the search words in the **Search Criteria** field. You can also use wildcard to make your search more specific.



In the screen shown above, the user has entered a wild card (% sign) after the word "California" and run the search. As a result the system showed all the alarm state definitions that starts with the word "California".

- 2 To view the entire **Alarm State Definition database**, click **Find Now** without entering any value in the search field.

Options

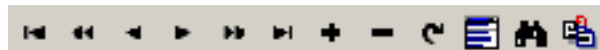
Under **Options** menu there are 6 choices. First four choices (Frame Settings, Load Multiple Images, Delete Frame, Add Frame) works only with **Animation Script Builder** tab. Next two options (Animation On, Transparency Color) will only be available when **Alarm State Definition** tab is active.

- 1 **Frame Settings** - Click this button to specify the number of frames and the height and the width of each frame.
- 2 **Load Multiple Images** - This option allows the user to select more than one images from the directory and load them into the frames.
- 3 **Delete Frame** - Click this option to delete frames.
- 4 **Add Frame** - Click this button to add frames to the screen.
- 5 **Animation On** - This option is available only when **Alarm State Definition** tab is active. This option allows the user to preview the icon or the animation file. Select the alarm state record and click on the Animation On option from the Options menu. You can also do this by right clicking on the alarm state record and selecting the Animation On option.

You can also change the **Animation Interval** by entering a value in the status bar. The interval is calculated in milliseconds. 1000 milliseconds = 1 second

- 6 Enter the value and click on **Apply Changes** button.
- 7 **Transparency Color** - Click this button if you want the image to be on a transparent background. You can preview the transparency effect by adding a background color to the icon or animation script attached to the alarm state record.

Toolbar



The different arrows on the tool bar allow you to move between alarm state records.

Click on the plus sign (+) to create a new record.

Click on the minus sign (-) to delete a record.

The curved arrow sign allows you to refresh the contents of the data set.

Click on the note pad sign to view the current record you are in (selected record). This feature is helpful, if you want to make changes to the selected record.

The binoculars sign represents the search feature. The search feature is equipped with an Advanced Find option, which enables the user to customize their search criteria.

The icon with two note pads and a red curved arrow allows the user to duplicate a record.

Advance Find

Using the **Advance Find**, the user can build the search criteria by selecting appropriate entries from the drop down list box and entering specific values in the value field. You have to select a specific field name, condition and a specific search value.

Advance Find uses **Boolean Logic** to create complex and highly precise searches. Boolean logic uses three connecting operators (Not, AND, OR) to narrow or broaden a search or exclude a term from the search. It is the process of linking criteria to narrow or expand a search through the use of **NOT, AND, or OR**.

Using Advance Find feature, the user can customize the search and save it for a later use. The saved search criterion is displayed only for the operator who defined it.

Alarm State Definitions or Alarm Template Definitions can be searched using field values like Alarm State ID, Caption, Animation File, Animation Interval, Frame Height, Width or Transparency.

To run a search using advance find option:

- 1 Click on the **Alarm State Definition** tab or **Alarm State Template Definition** tab. Then click on the binoculars located on the tool bar or click on the **Search** button and select *Find* from the drop down menu.
- 2 The **Search** window is displayed. Click on the **Advance Find** button located on the top right hand corner of the search window.
- 3 **Advance Find** window is displayed. Define your search criteria by selecting appropriate fields and conditions.
 - a) If you want to search for Alarm State ID = 10, you need to first select the left parenthesis and then select Alarm State ID as the Field name.
 - b) Enter (=) as the condition.
 - c) Enter the value as 10.
 - d) Close the right parenthesis.
 - e) Click the **Add to List** button.
 - f) If the criteria you defined is invalid, it appears in red font under the *Where Clause* section. If you would like to specify additional search conditions, select *And* or *Or* from the drop down box and define the next criteria.

Use of Wildcard

The Advanced Search feature provides ways to select certain Alarm State records without typing complete information. The **Schlage SMS** allows the use of wildcard (more formally known as metacharacters) to stand for one or more characters in a cardholder record. A wild card is a value entered into a query field that represents any other value and is usually used when exact values are not known. The users can do partial match searches by using the % (percent sign) as a **wildcard**. Within the search criteria, a user can type the % character before or after their search text as a wildcard

E.g. Entering % *secured* will return all the alarm states that end with the letters “*secured*”. By using the wildcard in the beginning, the user is requesting the system to find all parts that end with “*secured*” and could have additional characters in the beginning.

Entering %*secured*% will return all the records that contain the letters “*secured*”.

Wildcard has a very flexible capability to help users identify specific information based on limited or partial search information. One thing to note; however, this capability can result in very large query results if misused.

Alarm Graphics-Settings

CHAPTER 20

Introduction

Alarm Graphics Settings allows the user to customize the display of map names and icons in the navigation view window.

When an alarm goes off the maps and icon will be displayed in different colors that is set by the user to alert the operator about the new alarm.

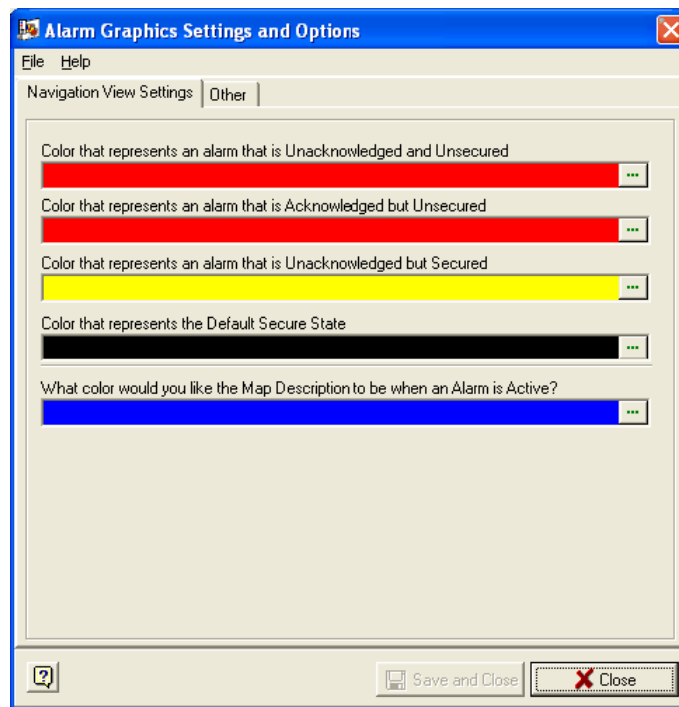
It also helps the user to define the size of the information box that provides additional information and functionality when an alarm is active or when there is no alarm in the buffer.

Navigation View Settings

Here the user can define colors that represent different alarm states. The user can also define how the map description should be displayed when an alarm is active.

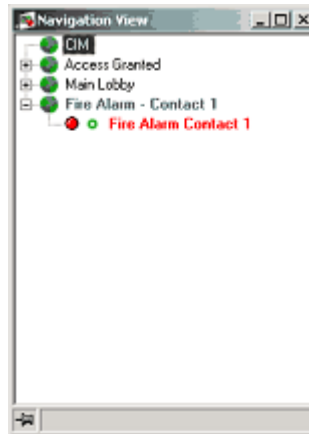
Follow these steps to define the settings.

- 1 Open the **Alarm Graphics Settings** program by double clicking on the corresponding icon in the **System Launcher**.
- 2 Select colors for each alarm state and map description by clicking the expand button.



- 3 When you click the expand button the color palette is displayed.
- 4 When the alarm is received, the corresponding map and icon description and information square will changes to the color that is selected here according to the alarm state.

- 5 See the screen capture shown below.



Information Box Setting

Each icon has several indicator boxes that provide additional information and functionalities. These boxes are different when alarm is active and when there are no alarms in the buffer.

The setting here simply defines the size of the box in pixels.

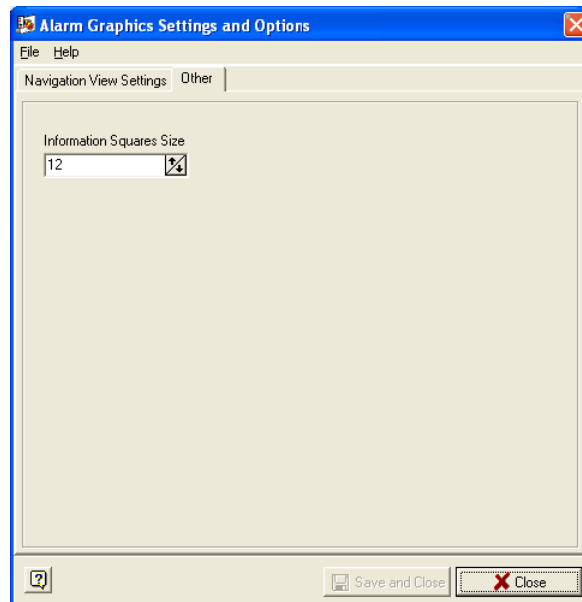


Icon Default State



Alarm Active State

- 1 Click on the **Other** button in the Alarm Graphics Settings window.



- 2 Enter a value between 12 and 32 to set the size of the information box. 12 is the default value and will display a small information square near the icon. 32 is the highest value that the system allows the user to enter.

Alarm Graphics-Editor

CHAPTER 21

Introduction

The user has to set up the program accordingly to attain the graphical representation of alarms. The user also has to attach live video, SVTR Playback and override tasks with the icons to access these features. The user defines maps, icons, and cameras, override tasks etc. using **Alarm Graphics Editor** program.

Alarm Graphics Edit program is always disconnected from the SP and will not receive alarm transactions. Only Alarm Graphics Client establishes connection to SP and receives transactions.

The operator must have Read/Write permissions to the system to perform the add, edit and delete functionality.

Setting up maps and icons

Before you start working with the Alarm Graphics - Editor, make sure that the program is added to the System Launcher. If you cannot find the icon for Alarm Graphics in the System Launcher, open the System Security module and add the program to the launcher. The procedure of adding programs to the launcher is described in the *System Security* Chapter.

Next, make sure you have Read/Write privileges to the program to set up maps and icons.

Create a New Map

Maps are graphical representation of locations within the secured area. Icons are placed in appropriate positions of these maps.

- 1 Login to the system using your assigned user ID and password.
- 2 In the **System Launcher** double click on the **Alarm Graphics** icon.
- 3 Select the **New Map** option from the **File** menu, or double click on the tool bar icon *Create a New Map*. The first step in inserting a new map, is adding a description and notes for the map file. The Description shall contain 64 alpha-numeric characters. The Notes field allows the user to enter 256 alpha-numeric characters.

Wizard to Insert a New Map

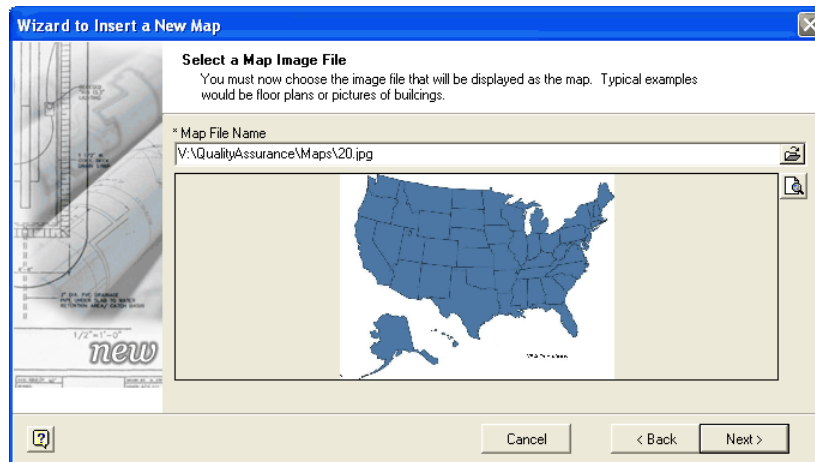
General Information
Please enter the Summary Description and any Notes on the new map being created. The Summary Description will appear throughout the application within hints.

* Description
USA Map

Notes

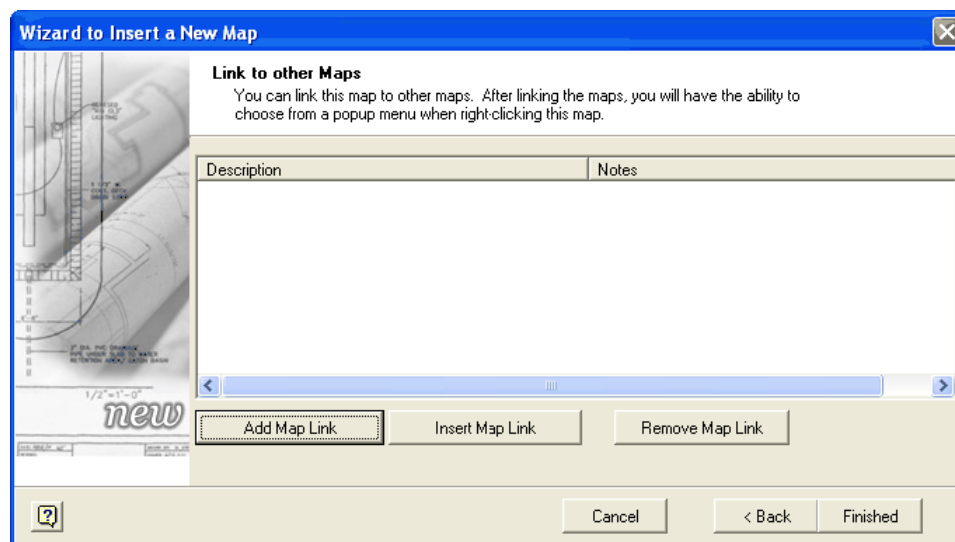
Cancel < Back Next >

- 4 Next, insert the map file. When you click the expand button by default, C:\Program files\Schlage\Data\Maps folder opens. If you don't have the appropriate file in that folder, select the file from your hard drive or network folders. You can see a preview of the map file in this window. You can open the image in a new window by clicking on the preview button located on the right hand side of the preview box. Click **Next** to continue or **Cancel** to cancel the process.



Note: The preview file is resized to fit in the box displayed in the window and will not be a true representation of the original image.

- 5 In the next step, you can create links to other maps defined in the program. This helps the user to navigate between all the maps defined in the system easily. All the maps linked here are available in the right click option of the map being defined. Click the **Add Maplink** button in the following window.



All the maps available in the system are displayed. Select the maps to which you want to add links, from the currently displayed list. The system allows the user to create unlimited map links.

The maps you selected here are displayed in the **Link to Other Maps** window. Click **Insert Map Link** you want to insert more maps or **Remove Map Link** to clear any of the map links.

If you click on **Insert a Map Link** button, the map will be inserted into the list, where as **Add a Map link** button will add the map to the bottom of the list.

Note: The user cannot create map link to the same map that is being defined or modified.

- 6 Click the **Finished** button to complete the adding new map process. Click the **Back** button to go back or **Cancel** to cancel the process.
- 7 Once you complete the **Add a Map** process by clicking on the **Finish** button, the map you added will be displayed in a new window.
- 8 You can define as many maps in the system, according to your company requirements.

Inserting icons on Maps

In **Alarm Graphics** Program, the user can associate icons with alarms, manual overrides, live video and SVTR camera playback.

Creating icons and animated graphics

The user can use any image as an icon. It is advisable to use logical graphics that represents a particular type of alarm. Schlage SMS also provides an application (Alarm State Builder) that helps the user to associate different icons with different alarm states (E.g. unsecured and unacknowledged). The Alarm State builder also helps the user to create custom animated graphics. Refer to **Alarm State Builder** for further details.

Steps to insert a New Icon

- 1 To add a new icon to the map, select the **New Icon** option from the **File** menu. You can also add the icon by double clicking on the appropriate tool bar icon.
- 2 The first step in inserting a new icon is to give a description to the icon, you are going to insert. The user can also enter notes for the icon.

The description should be limited to 64 alphanumeric characters and the notes should be limited to 256 alpha numeric characters.

Click on the expand button to select the destination map for the icon. This decides on which map the icon will appear. Initially the icon will appear on the upper left corner of the map. The user can move the icon to the desired location using a mouse.

The screenshot shows the 'Wizard to Insert a New Icon' dialog box with the 'General Information' tab selected. On the left is a sidebar with a map preview and a list of options: Insert, Item, Door, Alarm, Camera, Additional, Options, Modify, and Properties. The main area contains the following fields:

- * Description:** A text field containing 'NJ'.
- Notes:** A large empty text area.
- Destination Map for Icon:** A dropdown menu showing 'USA Map' with a green expand button (three dots) to its right.

At the bottom are three buttons: 'Cancel', '< Back', and 'Next >'.

Next, insert the image file that represents the icon's default state. By default state, it means the appearance of the icon when there is no alarm in the buffer. After that, select the maps to be displayed while selecting zoom in and zoom out options when the icon is in the default state.

Note: Selecting zoom in and zoom out maps are not required fields. These fields can be cleared by clicking the red X button located at the right hand side of these fields.

The screenshot shows the 'Wizard to Insert a New Icon' dialog box with the 'Default State' tab selected. The sidebar is the same as in the previous screenshot. The main area contains the following fields:

- Choose the animation when the Icon is in the Default State:** A dropdown menu showing 'CP - Fire Alarm - Default' with a green expand button (three dots) to its right.
- Close Map when alarm changes to the Default State?:** An unchecked checkbox.
- Zoom In Map when in Default State:** A dropdown menu showing 'Parsippany HIJ' with a green expand button (three dots) and a red X button to its right.
- Zoom Out Map when in Default State:** A dropdown menu showing 'New Jersey' with a green expand button (three dots) and a red X button to its right.

At the bottom are three buttons: 'Cancel', '< Back', and 'Next >'.

Check the box **Close the Map when alarm changes to Default State** to close the map, when the icon reverts to its default state i.e. there are no alarms in the buffer.

If this check box remains unchecked, the system will not close the map when the icon goes back to the default state.

Adding Alarm Labels

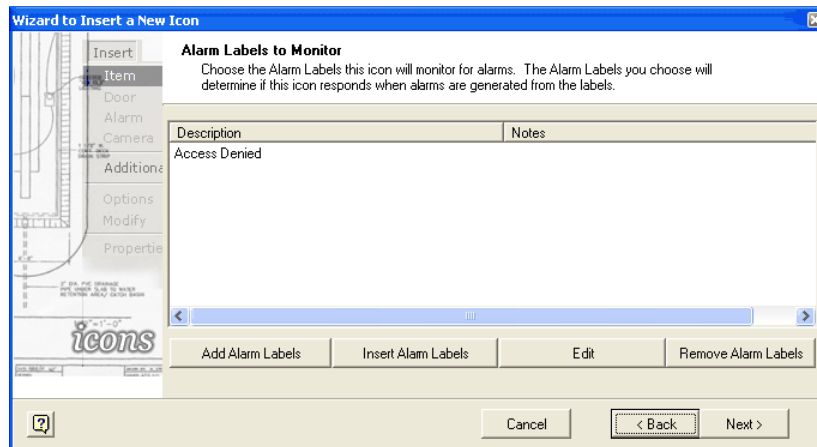
To receive real time display of alarms in the Alarm Graphics you need to attach the alarms label with the icons.

When a transaction occurs, the SP takes the transaction information and searches for transactions defined as alarms. Once the SP finds an alarm label, it generates the alarm. SP then retrieves the alarm label information to get the groups and workstations that are attached with the alarm. Once SP finds the workstations, it sends the alarms to specific workstations.

In order to receive alarms on the Alarm Graphic Workstation, you need to define that particular workstation in the alarm label definition.

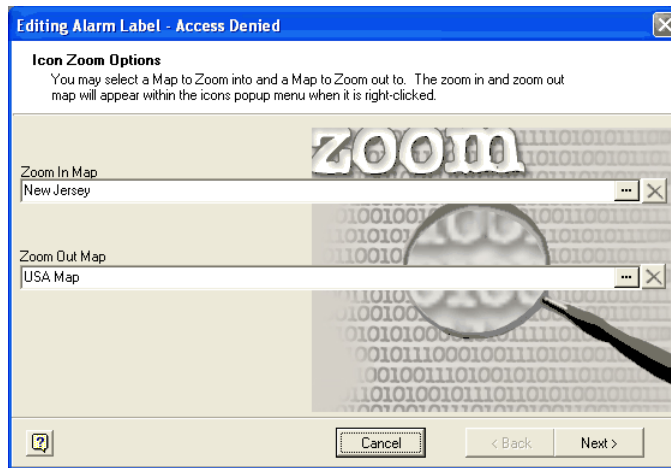
Then, you need to attach the alarms with the icons, so that you should be notified of the arms in the alarm graphic station. When any of the alarm that you have attached with the icon occurs, the icon will change its state to alert the operator about the existence of the alarm.

- 1 Select the alarm label for the icon by clicking the **Add Alarm Label** button.

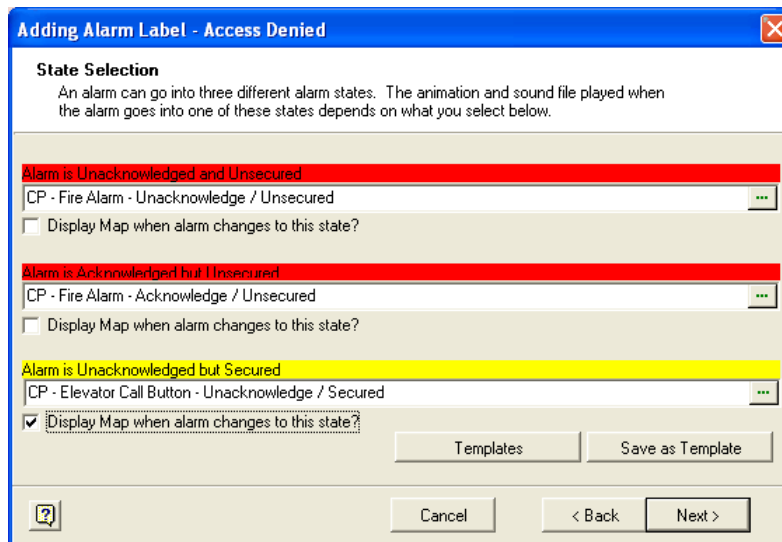


- 2 In the **Select Alarm Labels** window, all the alarm labels defined in the system are displayed. Select the labels that you want to attach to the icon.
- 3 Once you have selected the alarm labels required to attach with the icon, click **OK** to add them.

- 4 When you click **OK**, the **Icon Zoom Options** window is displayed. Here you need to select the maps to zoom in and zoom out when the selected alarm occurs.



- 5 Click **Next** to continue.
- 6 Now, select the graphics (animated graphics) to be displayed while the alarm is in different states.



- 7 Click on the expand button located on the right hand side of each field to select the graphics for each alarm states.
- 8 If you have defined alarm states as templates in your system, click on the **Template** button to select the appropriate template.
- 9 Click on the **Save as Template** button to save these Alarm State Graphics as template.
- 10 If you want the system to display the map when the alarm state changes to any of these, select the option **Display map when alarm changes to this state**.

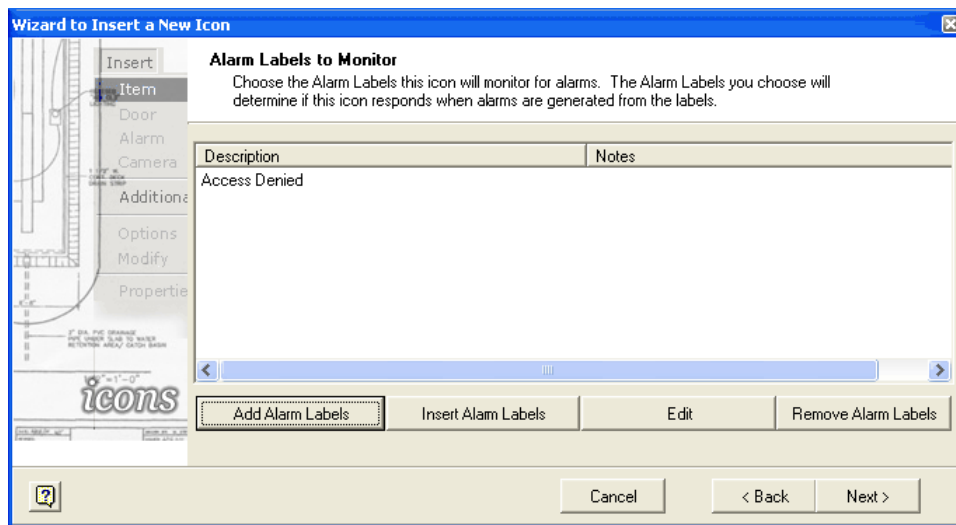
Note: If **Display map when alarm changes to this state** option is not selected, when an alarm occurs the corresponding map will not pop up.

- 11 Next, if there is a device attached with the alarm, add the device here.

If the user does not select any device, the system will add all the devices attached with the alarm in the system. For example if you have selected “Contact Active Alarms” the system will add all the contacts defined with that alarm as devices and the icon changes its state whenever any of the contact becomes active.

In order to receive alarms from a specific device only, the devices should be itemized in the alarm label definition. If you select a specific device and attach it with the icon, the icon changes its state only when a transaction (that is defined as alarm) occurs in that particular device. Here the icon works as a filter to the alarms.

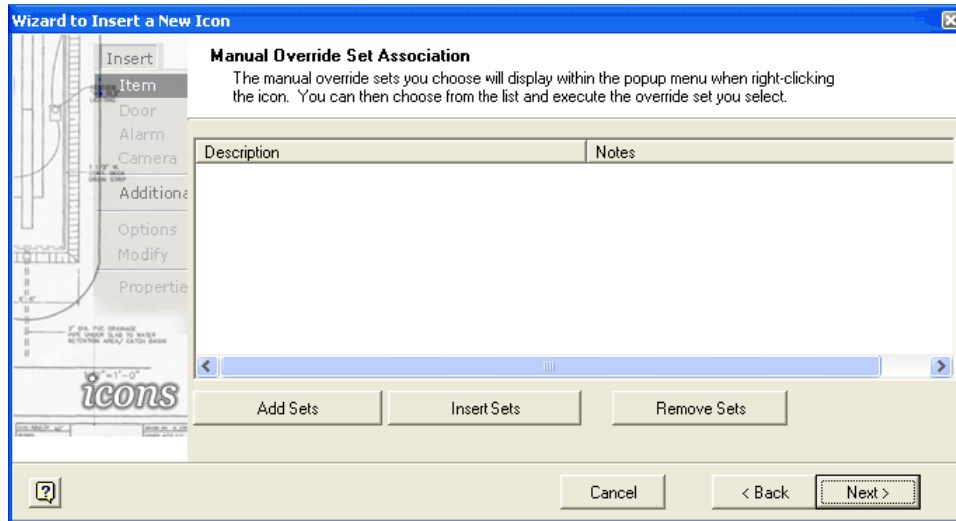
If it is a cardholder alarm (e.g. Access Denied) you can select and attach specific cardholders with the icon. Here also the icon changes its state only when the selected cardholder generates the alarm.



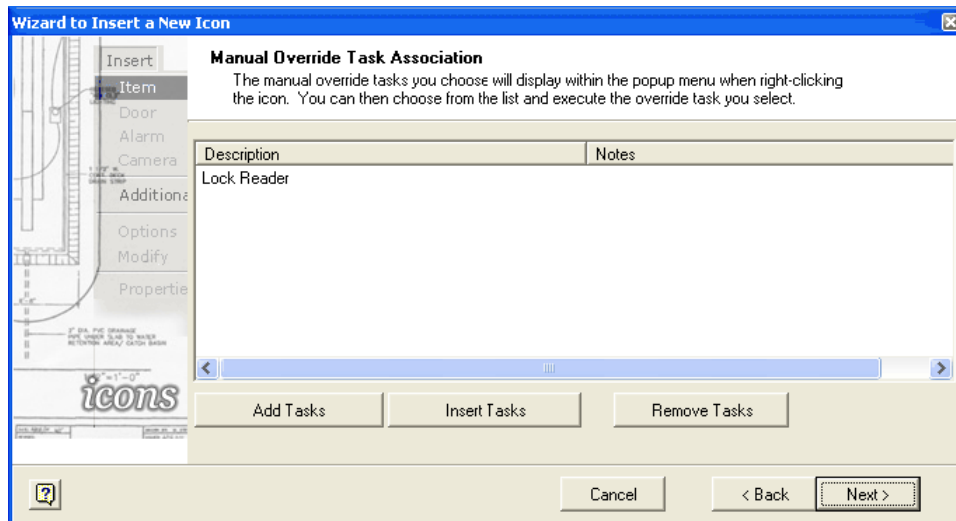
- 12 Click **Finished** to complete the process.
- 13 Like this you can attach as many alarm labels as you like with one icon.

Attaching Override Sets, Tasks and Camera Control

- 1 Once you have defined all your alarm labels, attach the override sets and tasks for a particular alarm label.

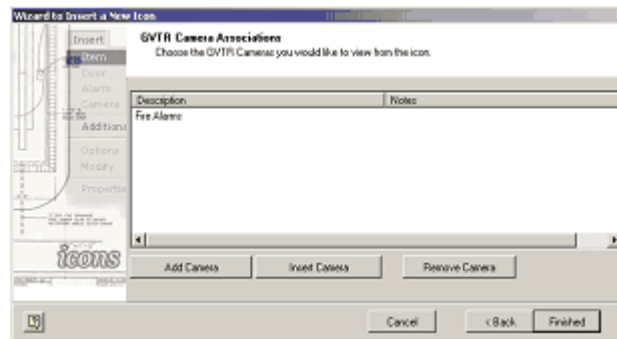


- 2 Click the **Add Sets** button and all the override sets defined in your system will be displayed in a separate window. Select the sets and click **OK**. Hold down the shift key to make multiple selections.
- 3 Click the **Insert Sets** button to insert override sets at a particular position. If you want to remove any override sets from the list, select it and click the **Remove Sets** button.
- 4 Next, you can attach override tasks with the icon.



- 5 **Add**, **Insert** and **Remove** buttons work in the same way as in the previous step.

- Next select the cameras you want to attach with this icon. You can access this camera by right clicking on the icon and this camera will display live video from the location of the camera.



Note: You must have SVTR installed in your system in order to enable this functionality.

- Click the **Finished** button to complete the process.

Like this you can define as many icons you want on a single map. Also, you can define icons in the map that you zoom into and attach alarm labels, override tasks and live video.

Editing a Map

- To edit an existing map either select and double click from the navigation tree or click on the tool bar icon.
- The **Edit** window is displayed. You can edit any of the previously entered information including, description, notes, map file and the map links. Click the **Finish** button to complete the editing.

Alarm Graphics-Client

CHAPTER 22

Introduction

The Alarm Graphics Client Module connects to the SP and receives alarm transactions. Maps and icons begin to respond to these transactions, based on how they are defined.

In order to receive graphical representation of alarms, the **Alarm Graphics Client** program must be added to the *Start Up* tab using **System Security** program. However, the system does not allow you to add both **Alarm Monitor (on page 282)** and **Alarm Graphics** to the **Start Up** tab at the same time. So, if you want to add Alarm Graphics program to the Start Up tab, you need to first remove Alarm Monitor from the Start Up.

Note: The operator must have at least Read Only permissions to the Alarm Graphics program, in order to see alarms, video or executing override tasks.

Alarm Notification

When a transaction is generated, and the SP finds an alarm label and attachment that matches the transaction, it generates a new alarm. Based on the alarm label information, the SP sends the alarms to appropriate workstations. To receive alarms in Alarm Graphics Workstation, the administrator has to define one particular computer that runs Alarm Graphics program as workstation, when the alarm labels are defined.

When the Alarm Graphics Workstation receives alarms, the program searches for icons that have the alarm label attached with it. When it finds the appropriate alarm attachment, it displays the respective map with the animated icon based on the definition, notifying the operator about the state of the alarm (E.G. Unacknowledged and Unsecured).

When an alarm occurs, the map is displayed showing the animated icon.



See that the icon representing New Jersey state is in red color representing an unsecured and unacknowledged alarm.

Alarm Acknowledgement

When an alarm occurs, the operator is notified with the graphical representation of the alarm state. Also if there is a sound file attached with the alarm, the system plays the sound file. The operator can access all the possible options from the right click menu of the icon.

The following screen capture shows the right click options available for an Access Granted transaction. These options varies based on the transactions and what options you have set while defining icon definition.

- 1 **Zoom In** - Click on this option to zoom into another map. This would be the map that is defined as the zoom in map when the alarm goes off. There can also be a **Zoom Out** map if it is defined in the system.
- 2 **View Alarm Details** - Clicking on this option opens the **Alarm Details** window. It is here that the operator acknowledges the alarm.

Alarm Details and Comments

Alarm Priority: 1

Alarm Date and Time: 5/15/2007 1:57:06 PM

Alarm Transaction: Access Denied - Badge not in controller memory

Secured: 5/15/2007 1:57:06 PM

Acknowledged: Unacknowledged

Acknowledged By:

Controller: Main board

Device: Rdr on Ch 3

Cardholder: 330: Anderson, Tom S

Operator: n/a

Description: n/a

Alarm Comments

Called security.

Comment	Operator	Date and Time
Called security.	Administrator, System	5/15/2007 1:57:44 PM

Insert Comment Insert Predefined Comment

Acknowledge Alarm Close

Alarm 1 of 1 Current User: USR

The following information is displayed in the **Alarm Details and Comments** window.

- a) **Alarm Priority** - This indicates the priority level of the alarm.
- b) **Alarm Date & Time** - The date and time the alarm has occurred is displayed in this field.
- c) **Alarm Transaction** - The transaction that caused the Alarm.
- d) **Secured**: Whether the device that is attached to the particular alarm is secured or not.
- e) **Acknowledged** - Whether the alarm is acknowledged or not.

- f) **Acknowledged by** - The name of the operator who acknowledged the alarm.
- g) **Controller** - The controller that is connected to the device which generated the alarm.
- h) **Device** - The device that generated the alarm. (E.g. In a situation where there is an alarm called "Lost Link to Reader", the Reader is the Device. The name of the Reader will be displayed in this field.)
- i) **Cardholder** - If the alarm is a cardholder alarm, the name of the cardholder will be displayed here.
- j) **Operator** - If it is an operator alarm (E.g. illegal login) the name of the Operator is displayed in this field.

The right hand side of the window contains instructions to the operator, the comments that are added by the operator and the Live Video of the device that is monitored.

Click on the **Alarm Instructions** button to see the instructions to the operator. These instructions are entered in the Alarm Definition program, when an alarm is defined. The administrator can also attach a .wav file with for each instruction.

Depending on how the alarm was defined, you may be required to provide User ID or comments for the highlighted alarm before the system accepts the acknowledgment command. The administrator can "*force login*" and "*force comments*" before letting an operator to acknowledging an alarm. If this is the case, the applicable window will open for you to enter said requirements and acknowledgment will be accepted.

Receiving video of alarms

If there is Schlage Enterprise Video Management System (**SEVMS**) attached to your **Schlage SMS**, you can receive video of certain transactions that occur in the system. The cameras and video servers are defined and attached to alarms using the **SVTR Camera Definition** (see "SVTR" on page 474) module. You can receive video of only cardholder (Access Denied and Access Granted) and contact transactions. The Alarm Monitor and Alarm Graphics programs are capable of displaying live and recorded video. The recorded video can also be displayed in a separate window so that the user can still view the live video while viewing the recorded video.

- 1 You can play the video by clicking on the **Play Video** icon on the main window of Alarm Graphics, Alarm Monitor and Transaction Monitor.

- 2 The video of the transaction from the camera is displayed on your monitor screen. This helps you to get potential information of all the alarms. You can perform the playback functionality using various buttons appear on the screen.



To receive video of transactions in the Alarm Monitor/Alarm Graphics, the user has to define the transactions, device that generates the transaction and the camera that is associated with it in the **SVTR** (on page 474) module.

The user also has to define transactions as alarms in the **Alarm Definitions** (see "Alarm Definition" on page 264) program to receive alarms.

You can also receive live video on the Alarm Monitor/Alarm Graphics while viewing the recorded video of a transaction. In the **Alarm Details** (see "Acknowledging Alarms" on page 284) window click on the button **Live Video/Recorded Video** button. The video from the camera associated with the transaction (alarm) is displayed on the screen. The order different tabs you see on the Alarm Details and Comments window can be changed by dragging the selected tab and dropping it in the desired location.



The left pane displays the live video and the right pane displays the recorded video of the transaction. The windows and tabs can be resized and the system saves the changes per user. The **PTZ** (Pan, Tilt, Zoom) **Control** allows you to view the different angles of the camera in the live video section. In the recorded video section, various buttons are available to play the video, stop the video, play the next frame, play the previous frame, begin the video and end the video. Move the mouse over these buttons to see the captions for each button.

Note: If the camera does not have PTZ capability, the PTZ Control is not displayed along with the live video. For more information about the controls available on PTZ Control panel, refer to the **SEVMS** manual.

Sorting tabs

Users can rearrange the order of the tabs on the Alarm Details and Comments window using the drag/drop feature. Click on a tab and drag it to the desired location.

PTZ Panel

The PTZ Panel is used for cameras that support the Pan, Tilt, and Zoom functionality. If the associated camera is a PTZ camera, this panel is available through the modules that show live/recorded video of transactions (Alarm Monitor, Alarm Graphics and Portrait Monitor).

The following are the different functions available on this panel. The green signal indicates that the PTZ control is connected.

Change the camera angle - Changing the camera angle is done using the different arrows that are shown on the panel. This can be also done using the <Home>, <PgUp>, <End> and <PgDn> buttons on the right side of the keyboard.

Focus - Use the up and down arrows to adjust the focus of the camera.

IRIS - Iris buttons allow for light adjustment of the camera. Iris is an adjustable diaphragm of thin opaque plates that can be adjusted by the + and - buttons so as to change the diameter of a central opening usually to regulate the aperture of a lens.

Zoom - You can enlarge or decrease the size of the image by clicking on the up and down arrow buttons.

Speed - Using the sliding bar, you can adjust the camera movement.

Moving the camera to a preset Location - To go to a pre-set camera location use the **Send** button, it opens the extended panel. Enter the number of the camera location and click **Enter**.

Setting a new location - To set a new location move the camera to the desired location and click on the **Set** button. It opens the extended panel. Enter a camera location number and click **Set**.

Note: This feature is not activated in the PTZ Panel available through **Schlage SMS** modules. In **Schlage SMS**, the camera positions are pre-set using the **SVTR Camera Control** (see "Working with SVTR Camera Control" on page 474) module.

Aux On - To run a pre-set Auxiliary tour use the **Aux** button. The green signal shows the PTZ control is connected.

Step - There are modes in which a PTZ camera can be operated. Using the continuous mode allows a smooth and continuous movement of the camera when using the moving panel or the arrows as explained above. Pressing either on the middle button in the moving panel, on the space bar, or on "5" on the right hand side of the keyboard stops the camera movement. The step mode brings about a non-continuous movement. Each step allows the camera to move 1000 milliseconds. In the image above the number of steps is two, therefore the camera moves to the requested direction a period of 2000 milliseconds, then it stops.

Extended Control

Note: Based on the camera specification the extended control is enabled. Example a Pelco Spectra III series camera supports the extended control.

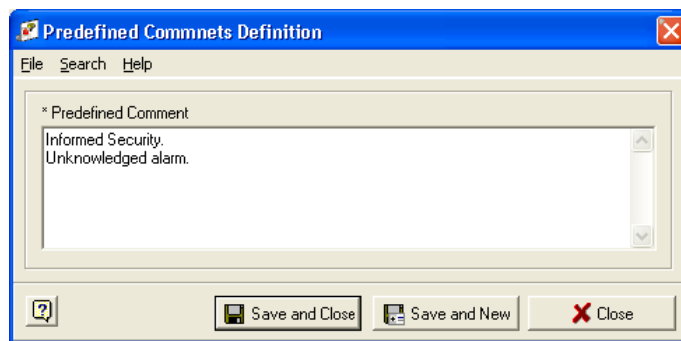
The **Auto Pan Stop/Start** button is used to pan the camera continuously until it is stopped. The **Set** pattern and **Pattern start** buttons are used to program and pan set patterns.

Pre-defined Alarm Comments

While entering comments you have the option to select the predefined comments or enter comments free- form.

Schlage SMS provides a program for the Administrator to set pre-defined comments for the operator to enter while acknowledging the alarms. Follow these steps to define alarm comments.

- 1 Open the **Pre-defined Alarm Comments** program from the System Launcher. To add new set of comments, click on the plus sign in the **Pre-defined Comments** window.
- 2 Enter the comments in the **Pre-defined Comments Definition** window.



- 3 Click **Save and Close** to save the application and return to the main window. Click **Save and New** to save the current definition and define a new one. Click **Close** to close the Definition window without saving the defined comments.
- 4 While defining alarms, the administrator can attach these comments with the alarm. The operator shall be able access these comments from the **Alarm Details** window while acknowledging the alarms.

Receiving Video of Alarms

If there is **Schlage Video Transaction Retrieval System** attached to your **Schlage SMS**, you can receive video of each transaction that occurs in the system. The **Alarm Graphics** program is capable of displaying live and recorded video. The recorded video is displayed in a separate window so that the user can still receive the live video while viewing the recorded video.

- 1 You can play the video by right clicking and selecting *Live Video* option on the icon located on the map.
- 2 You can also access the video from the **Alarm Details and Comments** window under **Live Video** tab.
- 3 In the **Alarm Details** window click on the button **Live/Recorded Video**. The video from the camera associated with the transaction will be displayed on the screen.
- 4 **View Recorded Video of this Alarm** button to play back the video of the alarm. This video file is opens in a new window called **SVTRPlay5** so that display of live video is not interrupted.

View Cardholder Image

Click on the button **Cardholder Images** from the **Alarm Details and Comments** window. The cardholder portrait and signature are displayed.



1 Preview Pending Alarms on this Icon

You can also view all active alarms that are routed to Alarm Graphics workstation. When you click this option these alarms (alarms for the selected icon only) will be displayed in Pending Alarms window.

Double click on these alarms to acknowledge them. The Alarm Details and Comments window is displayed.

You can also access the Alarm Details window from the right click menu of the alarm or the tool bar icon.

2 Find Alarm in the All Pending Alarms

When you click this option, the system highlights the alarm that you are viewing in the **All Pending Alarms** Window.

3 Executing Override Tasks

When an alarm occurs, the operator can execute necessary actions using the Override Tasks that are defined in the system. Each icon can have any number of manual override tasks associated with it.

Select and click on the task that you want to execute. The override task is executed as defined in the Manual Override Definition program.

Default State of an Icon

Alarm Graphics workstation is equipped with search feature for easily locating icons and maps especially when you have large number of items defined in your system.

- 1 Select **Find>Map** or **Icon** from the **Search** menu.

You can also access these by clicking on the respective tool bar icons that are available in the main tool bar of the program.



- 2 The **Search** window is displayed. Enter the name of the map or icon that you are looking for. Remember that you don't have to enter the name completely. If you enter the starting letters of the map, the system finds all the maps beginning with those words.

You can also put wild cards (percentage sign %) with the letters you are entering to find the maps or icons that contains those letters.

Use of Wildcard

The search feature provides ways to select certain records without typing complete information. The **Schlage SMS** System allows the use of wildcard (more formally known as *metacharacters*) to stand for one or more characters in a record. A wild card is a value entered into a query field that represents any other value and is usually used when exact values are not known. The users can do partial match searches by using the % (percent sign) as a **wildcard**. Within the search criteria, a user can type the % character as a wildcard before or after their search text.

Advanced Find

Using Advance Find, you can build the search criteria by selecting appropriate entries from the drop down list box and entering specific value in the value field. You have to select a specific field name, condition and a specific search value.

Advanced Find feature uses Boolean logic to create complex and highly precise searches. Boolean logic uses three connecting operators (NOT, AND OR) to narrow or broaden a search or exclude a term from the search. It is the process of linking criteria to narrow or expand a search through the use of **NOT, AND** or **OR**.

The Advance Find feature helps the operator to customize the search function. The operator can define the searches and save them for later use. The saved search criterion is displayed only for the operator who defined it.

Maps and Icons can be searched using fields like map ID, caption etc.

- 1 Click on the **Advanced Find** tab located on the top of the Search window.
- 2 The **Advanced Find** window opens.
- 3 To define the criteria, select the field name, condition and value. At least one criterion must be selected for the feature to work properly. When you run the search you will get the records corresponding to your search criteria.
- 4 Once you have defined the criteria click **File>Save**.
- 5 Add a description to your search and click **OK**. The new search will be saved and listed under the Advanced Find button.

Transaction Codes Editor

CHAPTER 23

Introduction

The administrator can customize the appearance of transactions based on the type of transactions. The font color, size, style, name and background color of the transactions can be configured easily.

Accessing the application

- 1 Open the System Launcher by double clicking on the **Schlage SMS** icon on your desktop or select Start>Programs>Schlage SMS>Schlage SMS.
- 2 Enter your assigned user ID and password.
- 3 In the System Launcher window, double click on Transaction Codes Editor icon.

Customizing Transaction Codes

The first thing the user must do before defining the Transaction Monitor is, customizing the color schemes for different transactions in the Transaction Codes Editor.

- 1 Open the Transaction Codes program and select the transaction you want to customize and double click on it.
- 2 In the **Transaction Codes Editor** window, there is a section named **Transaction Code Display Information**. Customize the Transaction Code by selecting a font color, size, style, name and background color appropriate for the particular transaction.

The screenshot shows the 'Transaction Code Definition' window. The 'Transaction Code Information' section includes fields for 'Transaction Code Hi' (2), 'Transaction Code Lo' (64), 'Description' (Access Denied - Badge has expired), 'Notes', 'Device Type' (Reader), 'Bitmap' (20), 'Secure Code' (0), and 'Secure Type'. The 'Transaction Code Display Information' section includes 'Font Color' (red), 'Background Color' (white), 'Font Name' (Arial), 'Font Size' (8), and 'Font Style' (Bold, Italic, Underline, Strike Out). A preview at the bottom shows a red transaction code '2 133' on a white background with the text 'This is an example of the transaction code display.' The window has a menu bar with 'File', 'Search', and 'Help', and buttons for 'Save and Close' and 'Close' at the bottom.

- 3 Select **File>Save and Close** to save the definition. Like this you can customize each transaction you have.
- 4 In the **Transaction Monitor** Program select **View>Reload Transaction Codes** to view the transactions in the newly defined style.

Transaction Filters

CHAPTER 24

Introduction

Filters are used to specify which incoming transactions you wish to see on the **Transaction Monitor** display. All transactions *other than* those included in a Filter will not be displayed when the filtering is enabled. All Filters and Filter Sets can be seen and edited in the **Online Monitor Filter Designer** window.

Accessing the application

- 1 Open the **System Launcher** by double clicking on the launcher icon on your desktop or select **Start>Programs>Schlage SMS>Schlage SMS**.
- 2 Enter your assigned user ID and password.
- 3 Double click on the **Transaction Filters** icon on the launcher window. The Online Filter Designer is displayed.

Defining Filters

The main window of the **Transaction Filters** module consists of three sections for creating and modifying **Filter Sets**, **Filters** and **Filter Attachments** to be employed by the Transaction Monitor.

The Tool bars in each section contain:

- Navigation arrows for locating records
- Insert New and Delete Current Record buttons
- Refresh button to bring most current data set
- Bookmark buttons
- View Current Record button to open the currently highlighted record for review or modification

Creating a Filter Set

The first step in creating filters is creating a filter set.

- 1 To create a Filter Set, click on the + icon in the Filter Sets section, and the **Filter Definition** window opens.

- 2 Enter the **Description** (name for the filter set) and notes about the filter and click on **Save and New** to start your next set or **Save and Close** when finished. Your new Filter Set will be listed on the top left of the screen.

Note: To add an existing Filter to an existing Set, click the check box next to the Filter Set that you want to add the filter to and then click on the **All Filters** filter set to choose from the whole list of Filters. Check the boxes for each filter and drag them over to the Set. You will be prompted to confirm the action.

Creating a Filter

- 1 To define a new filter, click on the **+** icon on the **Filters** section.
- 2 On the **Filter Definition** window enter a description for your new filter and notes associated with it. For example, we will create a filter for access granted transactions.
- 3 Enter the description as **Valid Access** and in the **Notes** field enter *Access Granted Transactions Only*.
- 4 Click **Save and New** to define another filter or **Save and Close** to complete the filter definition.
- 5 To select it, click the **+** icon under the Filters section and the Filter Definition window opens. Follow the same steps as done for the Filter Set. Your new Filter will be listed on the top right side of the window.
- 6 You can add the filter to the filter set you selected.

Attaching a Transaction to a Filter

The last step is to select the actual transactions that apply to the Filter you're creating and attach them to it.

- 1 To define filter attachments, go to the Filter Attachment section at the bottom of the Filter Designer window and click on the **+** icon. The **Filter Attachment Definition** window opens.
- 2 The description here should be named the same as the Filter you are attaching it to, as well as your notes.
- 3 In the Transaction Group field use the expand button or just click inside the field area. Then click on your selection and click **OK**.



- 4 Next, go to the Transactions field and in the same way open the **Select Transactions** window. All transactions that are defined for the transaction group you selected will be listed. Select the transaction(s) you want to include in your filter.

- 5 If the **Transaction Group** involves cardholders, go to the **Selected Cardholders** Field and click on the expand button. You will be prompted to save your changes. The Cardholders in Filter window opens. For individual selections, use **Add Cardholders** button to activate the **Cardholder Search** feature. You will receive an information message when cardholder selection is not required. Select the cardholder(s) you want to include.

Note: If you select **Add All Cardholders** option a warning message appears saying that this choice will delete any previously selected cardholders and replace them with one record representing All Cardholders. You can't undo this step, so be cautious when editing an existing filter.

- 6 Follow the same steps for selecting the devices. The **Devices in Alarm** window opens first and shows any existing record information. Choose Add Devices at the bottom to open the **Device Selection** window. This window will display only the devices that are associated with the transactions that you have chosen. Highlight a device and click **OK**. You should see the new record added to the Devices in Alarm window. Click **Close**.
- 7 After all selections are made, you will not see Cardholders or Devices listed in the Definition window. However, you may click on any field to open the related Selection window for details. Again, click **Save and New** or **Save and Close** to complete the process. Click on **Close** and then **No** if you don't want to save the new attachment (or changes) and you can begin again.

Editing Filter Definitions

- 1 To edit a filter, filter set, or an attachment, select the item and double click on it. The definition window open. Make your changes and click **Save and Close**.

Search

The search feature allows you to search and find filter sets, filters and filter attachment. Follow these steps to start your search.

- 1 Open the Generic search dialog by clicking on the binoculars.
- 2 Enter the search word in the search criteria field and click **Find Now**.

The search result shows all the records corresponding to the search entry.

Note: The system puts a * (wild card) after the search entry and search returns all the fields with the search criteria. For example in the screen shot shown above you can see the search criteria is the word "Access". The system returns all the records with the word Access.

Advanced Find

Using the Advance Find feature, you can build the search criteria by selecting appropriate entries from the drop down list box and entering specific value in the value field. You have to select a specific field name, condition and a specific search value.

Advanced Find feature uses Boolean logic to create complex and highly precise searches. Boolean logic uses three connecting operators (NOT, AND OR) to narrow or broaden a search or exclude a term from the search. It is the process of linking criteria to narrow or expand a search through the use of **NOT**, **AND** or **OR**.

The Advance Find feature helps the operator to customize the search function. The operator can define the searches and save them for later use. The saved search criterion is displayed only for the operator who defined it.

- 1 Click on the Advance Find button to open the **Advance Find** window.
- 2 Define the criteria you want to use.
 - a) If you want to search for Filter ID=10, you need first select left parenthesis from the list box.
 - b) Parenthesis can be used to create nested search clauses. Using the Parenthesis one can override the standard order of priority (left to right) for each Boolean statement in the search.
 - c) Select Filter ID as the Field Name.
 - d) Select equal to (=) as the condition.
 - e) Enter the value as 10.
 - f) Provide the closing parenthesis at the end.
 - g) If you would like to specify additional search condition you can select AND/OR from the list box.
 - h) If you enable the NOT check box the search result will display all the records except the ones mentioned in the NOT search criterion.

E.g. if you want to search Filter IDs between 10 and 20 and between 25 and 30 you can define the search criteria as follows. Use the double parenthesis to nest a search clause.

((Filter ID>10) AND (Filter ID<20))

OR ((Filter ID>25) AND (Filter ID<30))

When you run the search you will get records corresponding to Filter ID values 11 to 19 and 26 to 29.

- 3 When you are satisfied with the criterion, click **Add to List** button. If the criterion is not valid, it is displayed in red under the Where Clause section. When the criteria becomes valid the font color changes to black.
- 4 Once you have defined the criteria click **File>Save**.
- 5 Add a description to your search and click **OK**.
- 6 The new search will be saved and listed under **Advanced Find**.

Note: While defining your search criteria using a string, you can put a %(wild card) before and after your search word in the value field. Using% sign helps you to find all the fields with the search word.

For example if you want to search for all the records with the word "Access". In the value field you can enter "%Access%". When you run the search you will get the search result corresponding to the word "Access".

Transaction Monitor

CHAPTER 25

Introduction

The Transaction Monitor does a real time display of cardholder and device transactions. The user can set filters for certain transactions and save each Transaction Monitor separately. The user can screen out unwanted information by doing this. The program also allows the user to open multiple monitors simultaneously at the same workstations. With proper authorization, the user can access the Cardholder Definition, Previous Transactions and Transaction Filter Modules from the Transaction Monitor program as well. This enables the user to view Previous Transactions in one window while another window shows ongoing activity.

Accessing the application

- 1 Open the System Launcher by double clicking on the **Schlage SMS** icon from the desk top or select **Start>Programs>Schlage SMS>Schlage SMS**.
- 2 Enter your assigned user id and password in the Login window.
- 3 In the System Launcher window, select the **Transaction Monitor** icon and double click on it.

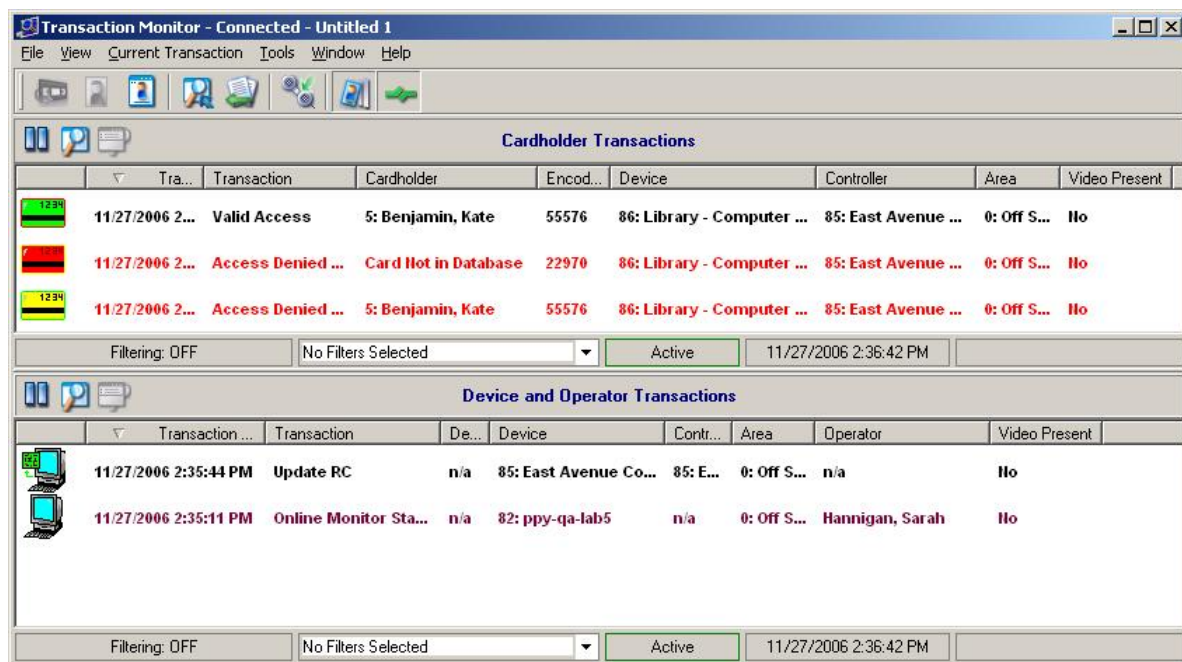
Working with Transaction Monitor

Overview

The **Transaction Monitor** window is divided into two panes. The upper pane displays Cardholder Transactions and the lower pane displays Device and Operator Transactions. The user can also view cardholder portraits and signatures for verification. In addition to that the User Defined Fields are also displayed in column, if they have been selected in the User Defined Fields Editor.

Using the Transaction Codes program all the transactions can be customized by font color, size, style, name and background color.

Note: The operators must have appropriate permissions to open the **Transaction Monitor**. Refer to the System Security section for further details.



Customizing Transaction Codes

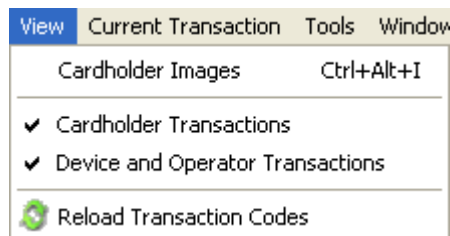
The first thing the user must do before defining the Transaction Monitor is, customizing the color schemes for different transactions in the Transaction Codes Editor.

- 1 Open the Transaction Codes program and select the transaction you want to customize and double click on it.
- 2 In the Transaction Codes Editor window, there is a section named Transaction Code Display Information. Customize the Transaction Code by selecting a font color, size, style, name and background color appropriate for the particular transaction.

- 3 Select **File>Save and Close** to save the definition. Like this you can customize each transaction you have.
- 4 In the **Transaction Monitor** Program select **View>Reload Transaction Codes** to view the transactions in the newly defined style. Otherwise the Transaction Monitor must be closed and reopened to display the new style you have defined.

Selecting a Transaction Group

In the Transaction Monitor window the user can either select to view Cardholder Transactions only or Device and Operator Transactions only or both.



You can also choose to show/hide transactions by clicking on the tool bar icons.



Show/hide cardholder transactions ←

Show/hide device and operator transactions ←

Saving Transaction Monitors

Once you have customized the monitor according to your needs, you can save it by giving a unique name. Like this you can define as many monitors as you like and save them separately. The system also supports multiple document interface which allows the user to open more than one transaction monitor at a time. All the saved monitors are protected by the operator login and those won't be available for another user.

Each saved monitors can have the following options saved.

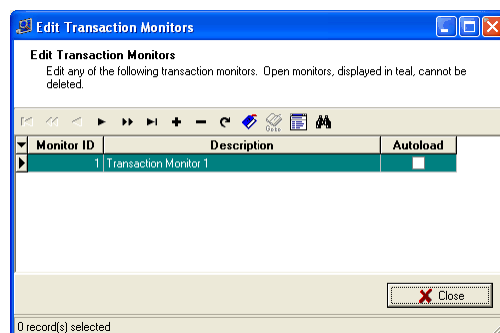
- 1 Viewing either Cardholder Transactions or Device and Operator Transactions or both.
- 2 The filters are enabled.
- 3 Cardholder image is displaying or not.
- 4 The option to pop up the transactions.
- 5 Auto-load the saved monitor when the Transaction Monitor program is first opened.
- 6 Set the number of transactions displayed.

Auto-load the saved Monitor

While saving a monitor you can set the option to auto-load the saved monitors when the Transaction Monitor program is first opened. Instead of opening an untitled monitor the program will open the monitors that you have saved as auto-load.

Editing Transaction Monitors

- 1 Select **Edit Transaction Monitors** from the **Tools** menu.



- 2 Double click on the monitor you want to edit. The monitor you have selected is displayed for editing.

Pausing Transactions

You can always stop the transactions being displayed in the transaction monitor by enabling the pause option.

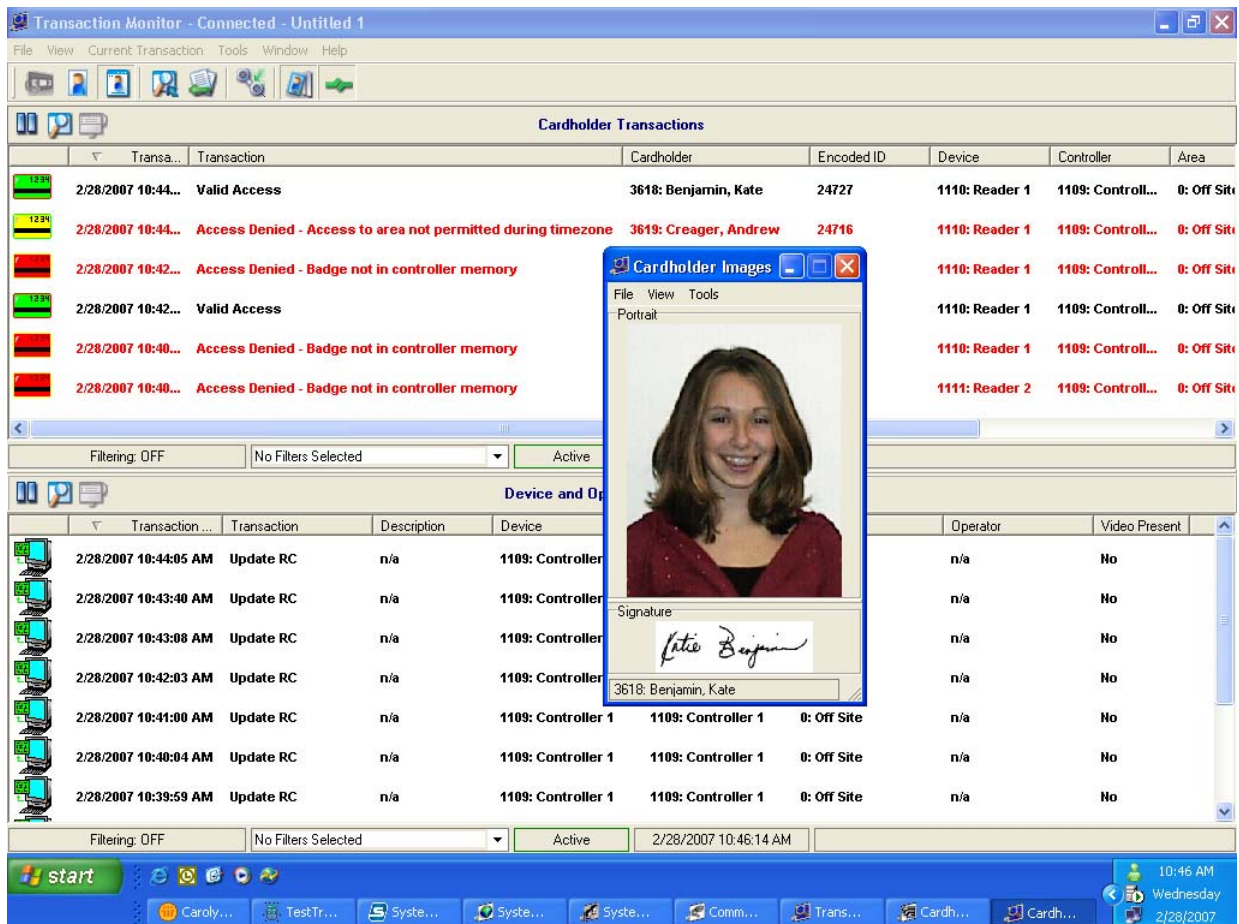
There are separate options for pausing cardholder and device and operator transactions. This helps the user to stop one particular transaction while the other continue to display.

- 1 Select **Fie>Pause Cardholder Transactions** to stop only cardholder transactions being displayed.
- 2 Select **Fie>Pause Device and Operator Transactions** to stop all the device and operator transactions being displayed.

Viewing Cardholder Portrait and Signature

If you are viewing Cardholder Transactions you can choose to view the Cardholder Portrait or Signature to reassure the security further.

- 1 Select **View>Cardholder Portrait** or Signature.



- 2 If you want to verify only the cardholder image, deselect **View>Signature** from the Cardholder Images dialogue.
- 3 If you want to verify only the cardholder signature, deselect **View>Portrait** from the Cardholder Images dialogue.
- 4 Selecting **View>Clear Images** option removes the images from the window.
- 5 To snap the Cardholder Images window to the corner of the computer screen, select **Tools>Options**. On the **Cardholder Images Preview Settings** window, select the *Snap Cardholder Images Window* checkbox and adjust the value using the up and down arrows.
- 6 To close the image preview dialogue, select **File>Close**.

- 7 You can also show/hide the portrait/signature preview window by clicking on the tool bar icon.



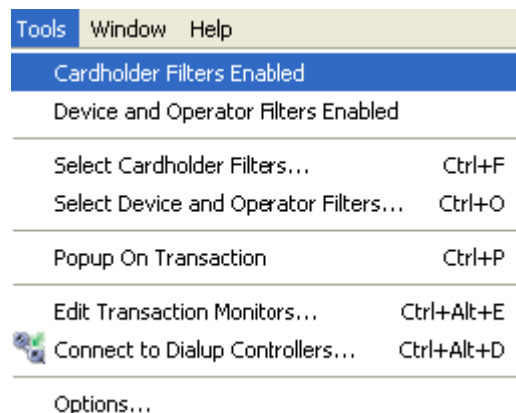
Playing video file of a Transaction

- 1 Select **Current Transaction>Play Video** to view the video of a transaction.

Filtering Transactions

The user can enable filters for cardholder or device and operator transactions or both. This feature allows the user to screen out unwanted transactions from the monitor. There are separate filters for Cardholder and Device and Operator Transactions.

- 1 If you want to enable filters for Cardholder Transactions only select **Tools>Cardholder Filters Enabled** option. A check mark appears indicating that you have enabled that option.



- 2 If you want to enable filters for Device and Operator Transactions select the option **Device and Operator Filters Enabled**.
- 3 Double click on the **Filtering On** button from the upper or lower pane depending on the type transactions you want to filter out. All the transactions corresponding to that group will be displayed. Select the transactions you want to filter and click **OK**.
- 4 Now only the transactions meeting these selected filters will be displayed.

Note: All the grids and columns that appear on the Transaction Monitor window can be resized and sorted by the user.

Pop-up on Transaction

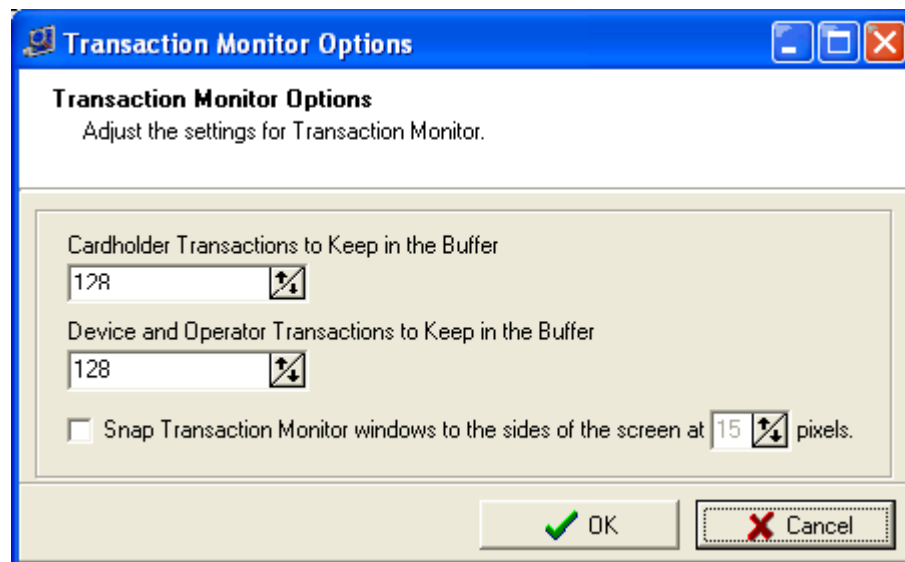
If you select **Pop-up on Transaction** option from the **Tools** menu the Transaction Monitor window will pop up automatically whenever a transaction occurs.

Note: Double click on the transactions to get an information tip showing all the information of the selected transaction

Options

The user can further customize the monitors by setting the number of transactions to be displayed on each Transaction Monitor that is saved.

- 1 Click **Options** from the **Tools** menu. The following window is displayed.

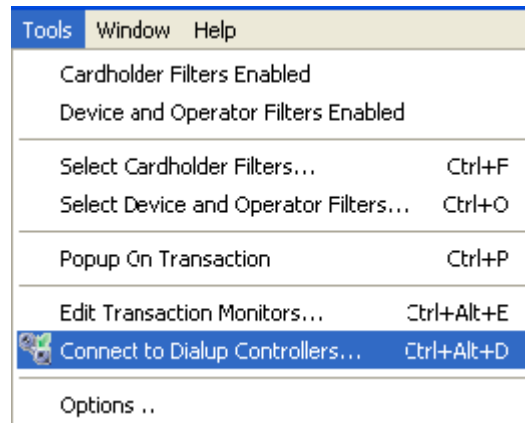


- 2 Enter the number of transactions you want to be displayed in the monitor.
- 3 You can also specify the number of pixels at which the **Transaction Monitor** window snaps to the corner of the screen.

Connecting to Panels via Dial-up

Transaction Monitor program allows the user to connect to the controllers located at remote locations using a dial-up modem and get transactions.

- 1 Select **Tools>Connect to Dial-up Controllers** menu.

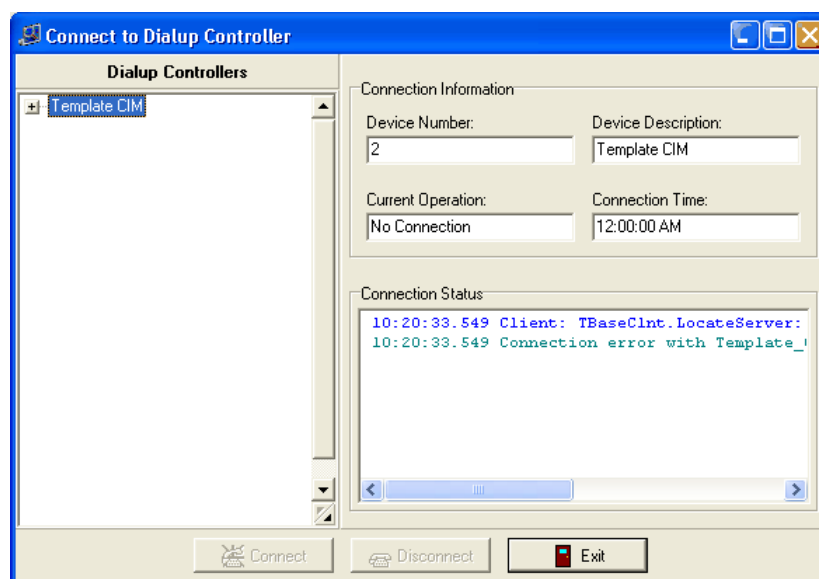


or click on **Connect to the dial-up controllers** icon to select the device.



Connect to dial-up controllers

- 2 The following window is displayed.



- 3 Select the device and click **Connect**. The CIM dials the controller specified and gets the recent transactions.

Viewing Previous Transactions

- 1 Select **View Previous Transactions** option from the **File** menu.
- 2 Enter the transaction type, day that transactions occurred, start and end time of the transactions etc.
- 3 Click on the **Run Report** button to run a report of the transactions you selected.

Accessing other applications from Transaction Monitor

Cardholder Definitions

You can access Cardholder Definition program from the Transaction Monitor to view or edit cardholder records pertaining to the transactions.

Select the **Cardholders in Cardholder Definition** from the **Current Transactions** menu.

Transaction Filters

You can access Transaction Filters program from the Transaction Monitor.

Select **Edit Transaction Monitor Filters** from the **File** menu.

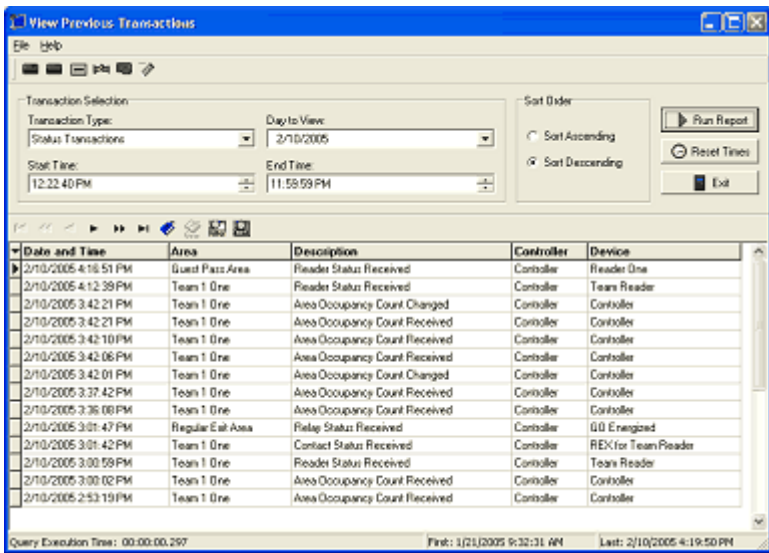
Previous Transactions

CHAPTER 26

Introduction

The **View Previous Transaction** module will provide an account of any transactions in the database. You can select which transaction type you want to view, the date, time and the sorting order to be displayed.

The main screen consists of the menu and tool bars, transaction selection, sort order and report controls, display grid, navigation bar, and status bar. Details follow for all screen features.



Accessing the application

- 1 Open the system launcher by double clicking the launcher icon on your desktop or select **Start>Programs>Schlage SMS> Schlage SMS**.
- 2 The login window, opens. Enter your user ID and password.
- 3 In the System Launcher window, double click on **Previous Transactions** icon.

Working with Previous Transactions

Running a Transaction Report

- 1 First select the **Transaction Type** from the drop down list. Drop down menu offers all system Transaction Groups to choose. You can only choose one transaction type at a time
- 2 Next choose the **Day to View**. By default it will be the current date. To change this, click on the down arrow to open the calendar. A red circle will appear around the current day.
- 3 Now set the **Start Time**. The default is set until you change it. To change this manually for the current report, click on the hour, minute, or second to highlight it and use the up and down arrows or type in the field.

Note: When you change the start time manually, the end time will set to 11:59:59 PM and has to be changed manually if necessary.

- 4 Set the **End Time**. The default is set at the current time. Changes are made the same as with Start Time. Select **File>Display Defaults** to change the defaults for the current reporting time periods. The system defaults are set to: Start 30 minutes prior to current time and End at current time, shown below.
- 5 Specify the **Sort Order**. Choose ascending or descending.
- 6 Click **Run Report** to begin the report. The fields of information returned from the history database tables are displayed in the **Display Grid**. This information may vary slightly depending on the type of transaction selected.
- 7 The **Reset Times** button resets the time to the default you have defined
- 8 Click **Exit** to closes the View Previous Transaction window.

Note: In the Status Bar the **Query Execution Time** at the left is simply the time it took for the query to run and return the selected report information. At the right, the First and Last fields are the dates and times of the first and last entries in the database transaction history table.

Printing the screen

- 1 Select **File>Print Screen** to send the current screen to designated printer.

Tool bar icons

Only the most commonly used transaction types have icon buttons. For more choices, use the Transaction Type drop down menu.

Note: When you click on one of these buttons, the Start and End time will be reset to the default, any current display will be cleared, and transactions occurring within the default start and end time will be reported immediately.



(In order of appearance from left to right)

- Access Granted
- Access Denied
- Reader Communications
- Contact Transactions
- Reader Controller Transactions
- Operator Actions

Transaction Type Definitions

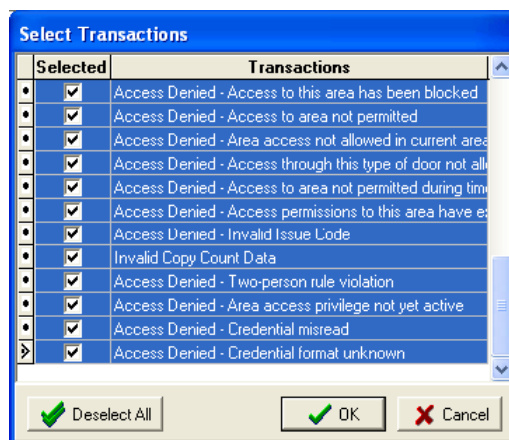
There are several Transaction Types available to choose from. Descriptions of them follow.

Note: As the list progresses, we will only detail differing items of information for each group.

- 1 **Access Granted Transactions** - Transactions include valid access, entry, exit and copy machine access. The report returns the following information:
 - a) **Date and Time** - of the transaction – returned for all transaction types
 - b) **Description** - the transaction that took place – returned for all transaction types
 - c) **Encoded ID** - the encoded ID number of the card used in the transaction (This can only be seen if the operator has permission to view encoded ID numbers.)
 - d) **Cardholder** - the name of the person ID card is assigned to
 - e) **Area** - location transaction occurred in – returned for all transaction types
 - f) **Controller** - the defined name of the Controller that reported the transaction
 - g) **Device** - the defined name of the Reader on the Controller that reported the transaction.
 - h) **Archive History** - This displays Archiver transactions and status.

Note: Current versions of **Schlage SMS** do not implement this feature.

- 2 **Access Denied Transactions** - Transactions include all those found in the Access Denied group.



- 3 **Reader Communications** - This reports any disruptions or restorations in the communications between the Reader Controller and the Reader interface. The report returns the following:
 - **Description** – Lost or Restored link transactions
 - **Reader** - the defined name of the Reader on the Controller that reported the transaction
- 4 **Contact Transactions** - These are specific changes detected in the normal monitored state of an input (i.e. motion detectors, doors, etc.). The report returns:
 - **Description** – the transactions relate to contact points only.
 - **Contact** - the number of the contact on the reader controller that reported the transaction, and the description of the device, typically the location of the contact point.
- 5 **Slave Controller Communication** - This option reports on the status of the connections between the Master Controller and the Slave Controllers. The following information is returned:
 - **Description** – Lost or Restored link transactions
 - **Controller** - The defined name of the Slave controller board
- 6 **Reader Controller Transactions** - This displays status messages originated by the Reader controllers. The report contains the following:
 - **Description** - of controller occurred during the transaction
- 7 **Operator Transactions** - This gives a report of the system activities of defined Operators and the workstations that they are using. These items are returned:
 - **Description** - Operator activity on the system
 - **Operator** - the user ID of the person using the workstation
 - **Workstation** - the name of the workstation
- 8 **CIM to RC Communications** - Transactions relating to communications between the CIM and the attached Reader Controller are returned. The Reader Controller will store information on expired badges and access records for 48 hours after expiration for the purpose of advanced notice prior to record deletion. These two types of transactions are newly included in this group.
- 9 **CIM and SP Status Messages** - This option displays transactions involving the status of the CIM or SP. The information includes:
 - **Workstation** - which workstation the message came from
- 10 **Download/Update Status Messages** - These transactions are related to system information downloads or updates from the CIM to the Controller.
 - **Description** - Reports whether update or download was sent to the reader controller
- 11 **Device Control** - This option relates to transactions during which an operator performs any type of Manual Override to a specific device.
- 12 **Guest Pass Transaction** - The transactions occur while using the Guest Pass System is called Guest Pass Transactions. The following is the list of transactions.
 - Guest Signed In
 - Guest Authorized
 - Guest Signed Out
 - Guest Reset to Pending
 - Guest Deleted Tour System Alarms
- 13 **Status Transactions** - You can view the following status transactions from this module.

- Reader Status Received
- Relay Status Received
- Contact Status Received
- Area Occupancy Count Changed
- Area Occupancy Count Received

14 Relay Transactions

- Relay Energized and Relay Released

Security Tour System Transactions

Tour System Transactions

1 Security Tour System Transactions

- a) **Tour Operator Transactions** - The following are the Tour Operator Transactions that can be defined as alarms.
 - Tour Started
 - Tour Stopped
 - Tour Resumed
 - Tour Paused
 - Tour Finished with Fault
 - Tour Finished Successfully
 - Tour Timed Out
 - Tour Out of Sequence
- a) **Tour Reader Transactions** - The following are the Tour Reader Transactions that can be defined as alarms.
 - Arrived On Time At Reader Checkpoint
 - Arrived Early At Reader Checkpoint
 - Arrived Late At Reader Check Point
 - Reader Checkpoint Never Reached
- a) **Tour Contact Transactions** - The following are the Tour Contact Transactions that can be defined as alarms.
 - Arrived On Time At Contact Checkpoint
 - Arrived Early At Contact Checkpoint
 - Arrived Late At Contact Check Point
 - Contact Checkpoint Never Reached

Manual Overrides

CHAPTER 27

Introduction

Manual overrides help the operator to change a device's normal state in case of emergency. The manual overrides can be programmed using the **Manual Override Definitions** program. All the programming for override sets, tasks and actions are completed in order to execute necessary actions by authorized operators. The range of actions is limited only by the security permissions granted to the individual (operator) or security group in the System Security program.

Accessing the application

- 1 Open the System Launcher by double clicking the **Schlage SMS** icon on your desktop or select **Start>Programs>Schlage SMS>Schlage SMS**.
- 2 The login window, opens. Enter your user ID and password. In the **System Launcher** window, double click on Manual Overrides icon.

Programming Manual Overrides

Overview

The main window of the **Manual Override Definition** program is divided into three sections. They are Manual Override Sets, Manual Override Tasks and **Manual Override Actions**. Tool bar icons are provided separately for each sections to perform various actions. Each grid contains standard navigation, Add\Delete\Refresh, Bookmark, Filter, Search and Edit record buttons.

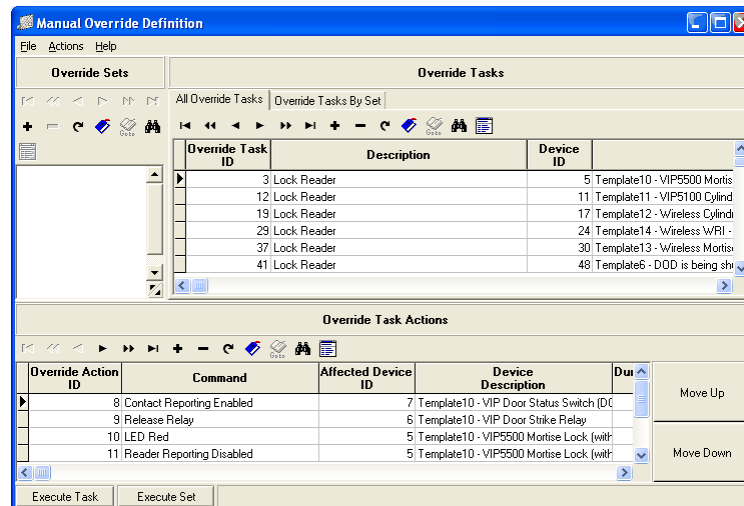
Defining Manual Override Sets

The **Override Sets** are created to organize similar tasks. For example, unlocking doors momentarily for non-employee visitors or for deliveries in different areas of the building. Tasks can be viewed quickly for selection and execution. An entire Set may be executed in the event of an emergency to unlock all the doors in the building in case of an emergency.

Follow these steps to define an **Override Set**.

- 1 Click on the + icon located under the section **Override Sets** to open the **Override Set Definition** window.

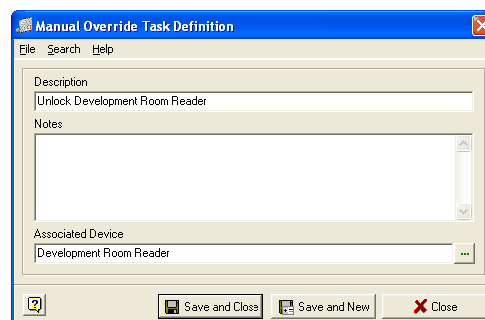
- 2 Enter a description (name) and notes (what type of override tasks will be included here). Click **Save and Close** and the new Set will display with a blank check box to its left in the Sets grid. Click **Save and New** to save the current record and define a new one. Clicking **Close** will close the window without saving the information.



Defining Manual Override Tasks

The Override tasks are defined in this section and later organized as Override Sets. There are two tabs in this section:

- **All Override Tasks** - New Override Tasks are created under this section. This default tab displays all existing tasks defined system.
 - **Override Tasks by Set** - All tasks included in the currently selected Override Set are listed here
- 1 Follow these steps to define an Override Task.
 - 2 Click the + icon to open the **Manual Override Task Definition** window. Enter a description and notes. Next select the device that is associated with this Override Task.

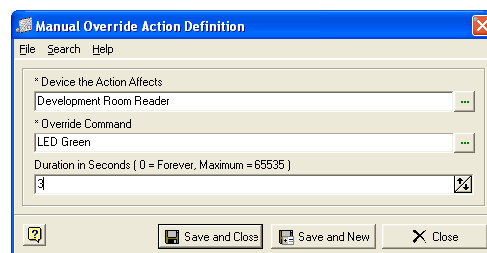


The Reader, Relay, Contact Selection window shown below contains tabs for Controller and Area Tree, as well as for each device type (the Reader tab is the default). All the devices defined in your system will display in this window. You may navigate through the Tree tabs or make your selections directly from the device type tabs. Click to highlight the appropriate device and click **OK**. Your selection appears in the Associated Device field. Then click **Save and New** to create another record, **Save and Close** or just **Close** to exit the function without saving any changes.

Defining Manual Override Actions

The next step is programming the actions for devices to take by defining commands. This section displays the Override Action ID, Command, Affected Device ID, Device Description and Duration in Seconds information.

- 1 Click the + icon in this tool bar to open the **Manual Override Action Definition** window.



- 2 **Device the Action Affects** - the expand button opens the **Reader, Relay, Contact Selection** window shown previously. Select a device by clicking on it. There are usually multiple devices with associated commands involved in completing an Override Task.

For example to open a door for a limited period of time you need to define actions for all the devices attached to the door such as a contact (disable contact reporting and trigger), relay (Energize relay) and reader (turn LED Green).
- 3 The **Override Command** button opens the **Select an Override Command** window. Two columns in here will display the Command ID number and the Command Description. The commands vary depending on the device you selected. You may search for a specific command by typing it in the incremental search section at the top of this window. The Commands are directly associated with the selected Device to be affected and the choices will differ accordingly.
- 4 Enter the **Duration in Seconds**. This is the length of time that you want the Override State to last. In other words, the door will remain unlocked or out of its normal state, for a number of seconds you define. The default is zero, which equals forever.

Note: You can set a duration for Manual Override Tasks if the Override Task has Override Actions that only affect a contact. The Override Action duration of the Task must be set to zero in order for this option to be available. Please refer to the **Timed Override Task and Set** (on page 362) section for details.

You may edit the records in any section by both highlighting and double clicking in its grid, double clicking on the record itself or highlighting and clicking the edit icon.

Attaching Tasks to Sets

As mentioned earlier in this section, **Tasks** such as emergency unlocks of all exit doors throughout a building may belong to one Override Set. In this case an entire Set can be executed at once. For the authorized Operator who will be performing these overrides it is also a more efficient means of locating particular Tasks. The final step in programming the manual override is placing your Task within a Set.

- 1 Select the box next to the **Set**, click to highlight the Task you want and drag the **Task** into the **Set**.

- 2 You will be prompted to confirm the action.
- 3 To view all the **Tasks** attached to a **Set**, select a **Set** from the list and click on the **Override Tasks** by Set tab in the Override Tasks section.

Edit

- 1 Double clicking on a record opens the corresponding definition window. Make your changes and click **Save and Close**.

Executing Override Tasks and Sets

- 1 To execute an **Override Task or a Set**, select a Task or a Set and click on **Execute Task** or **Execute Set** at the bottom left of the screen. These options are also available in the **Actions** menu.

Note: You need to have at least Read-Only permissions to the Area to execute a manual override set or task.

If an Override Task has Override Actions that only affect a contact and those Override Actions have a duration set at zero, users can set a specific duration for such overrides. Please refer to the **Timed Override Task and Set** (on page 362) section for details.

- 2 The Transaction Monitor and the View Previous Transactions programs display the following operator transactions whenever a manual override task or manual override set is executed.
 - **Manual Override Task Executed**
 - **Manual Override Set Executed**

Note: Utilize the navigation arrows, **Search** and **Filter** buttons to locate records more easily.

Examples of commonly used MRO procedures

The following are some of the commonly used Manual Override procedures.

- 1 Momentary lock
- 2 Lock forever

Momentary unlock

Follow these steps if you want to unlock the doors momentarily using a **Manual Override**.

- 1 First step is defining an **Override Set** that is going to include all the **Override Tasks** that will cause the doors to unlock for a definite period of time.
- 2 Open the **Manual Override Set Definition** window. Create an **Override Set** called "Momentary Unlock All Corporate Offices".
- 3 Define the **Override Tasks** that will include in this **Set**. (E.G. Momentary Lock Proximity - Corporate Main Entrance 1). Select the reader that is attached to the door as the device.
- 4 Define the actions that are going to cause the door to unlock.

- a) The first action is to disable contact reporting. Select the contact that is attached to the door you want to unlock momentarily. (E.G. Corporate Main Entrance DOD 1). Select the command **Contact Reporting Disabled**. Enter the duration for 30 seconds. This prevents an alarm being sent for the duration of 30 seconds while the door is open. Click **Save and New**.
 - b) Next, you need to define action for disabling contact trigger. Select the same contact you selected in the previous step. Select the command **Contact Trigger Disabled**. Enter the duration for 30 seconds. Click **Save and New**.
 - c) Next action is to energize the relay. Select the corresponding relay as the device. (E. G. Relay 1 - Main Entrance). The command is **Energize Relay**. The duration is for 5 seconds. Click **Save and New**.
 - d) The final action in this section is to turn the LED green. Select the reader that controls access through the door as the device. (E.G. Corporate Main Entrance 1 - Proximity). The duration is for 5 seconds. Click **Save and Close**.
- 5 Define Override Tasks for other doors you want to unlock momentarily at the same time. Drag and drop all the Override Tasks into the Override Set you created. Here the Set is "Momentary Unlock All Corporate Offices".

Reset momentary unlock

Follow these steps to reset the momentary unlock.

- 1 Define an **Override Set** called "Reset Momentary Unlock - All Corporate Offices".
- 2 Then define the **Override Tasks** for each door that is included in the Set. (E.G Reset Proximity - Corporate Main Entrance).
- 3 Then define the actions. First you need to reset the contacts. Select the contact that you shunt in the Lock Forever section as the device. For this example select "Corporate Main Entrance DOD 1". Now select the override command Contact Reset (all).
- 4 Next, you need to reset the relay. Select the relay and select the command Relay Reset.
- 5 Then reset the LED. Select the reader and choose the command LED Reset.
- 6 Executing this **Override Task** will reset all the devices (Contacts, relay and reader) attached to the "Corporate Main Entrance" to their initial state.

Unlock forever

Follow these directions to unlock the doors for a longer period of time.

- 1 For example create an **Override Set** called "Unlock All Corporate Offices".
- 2 Now create Override Tasks that will be a part of this Set. For example let us create an Override Task called "Unlock-IR Corporate Main Entrance". Select the reader that is attached to the door as the device.
- 3 Next step is to define the actions that will cause the door to unlock. The first action is to disable contact reporting. Select the contact that is attached to the door you want to unlock as the device. E. G. "DOD -IR Corporate Main Entrance." Select the command **Contact Reporting Disabled**. Leave the duration as zero(0). Click Save and New.
- 4 The next action is to disable the contact trigger. Select the same contact you selected in the previous step. Select the command Contact Trigger Disabled. Leave the duration as zero (0). Click Save and New.
- 5 Now define the action that energizes the relay. Select the corresponding relay as the device. E.G. Relay 1 -IR Corporate Main Entrance. Select the command Energize Relay. Leave the duration as zero(0). Click Save and New.

- 6 The final action is to turn the LED green. Select the reader. E.G. "Proximity -IR Corporate Main Entrance." Select the command "LED Green". Click **Save and Close**.
- 7 Create Override Tasks for all the doors you want to unlock at the same time and include them in the Override Set you created.

Reset devices

Follow these steps to reset the devices to their initial state.

- 1 Define an Override Set called "Reset Unlock - All Corporate Offices".
- 2 Then define the Override Tasks for each door that is included in the Set. (E.G Reset IR Corporate Main Entrance).
- 3 Then define the actions. First you need to reset the contacts. Select the contact that you shunt in the Lock Forever section as the device. For this example select "DOD -IR Corporate Main Entrance." Now select the override command Contact Reset (all).
- 4 Next, you need to reset the relay. Select the relay and select the command Relay Reset.
- 5 Then reset the LED. Select the reader and choose the command LED Reset.
- 6 Executing this Override Task will reset all the devices (Contacts, relay and reader) attached to the "IR Corporate Main Entrance" to their initial state.

Momentary lock

The following are the steps you need to follow to program Manual Overrides to momentarily lock the doors in an Area.

Note: The information used in these steps are only for instructional purposes. The actual data may vary depending on your business requirements.

- 1 The first step you need to do is create an **Override Set**, which includes all the tasks for Momentary Unlocks for all the doors in a building (or different buildings) or an Area.

For example we can create an **Override Set** called "Momentary Lock for All Corporate Offices". Enter your description and notes attached to it.
- 2 Now you need to define the **Manual Override Tasks** for this Manual Override Set. Click on the + sign to open the Manual Override Task Definition window. Enter the description and notes. Select the reader you want to lock momentarily as the device. For this example let us select "Proximity - Corporate Main Entrance". Click **Save and Close**.
- 3 Next step is defining the actions that will cause the door to unlock for a certain period of time. Open the **Manual Override Action Definition** window by clicking on the + sign at the lower part of the main window.
 - a) First action is to enable contact reporting so that opening the door during the time specified in the duration field will create an alarm.
 - b) Select the contact attached to the door you want to lock in the **Device that Action Affects** field. For example we can select "IR Corporate Main Entrance DOD".
 - c) Next select the override command, **Contact Reporting enabled**.
 - d) Enter the duration for 30 seconds.
 - e) Click **Save and Close**.
- 4 The second action is to enable contact trigger. Follow the same steps did in the previous step.

- a) Select the same contact (for this example "IR Corporate Main Entrance DOD") you selected in the previous step in the **Device that Action Affects** field.
 - b) The override command is **Contact Trigger Enabled**.
 - c) Enter the duration for 30 seconds. You can increase or decrease the duration depending on your specific needs.
 - d) Click **Save and Close**.
- 5 Next program the action to energize the relay attached to the reader that provides access to the **Area**.
- a) Select the relay that is attached to the door in the **Device that Action Affects** field. For this example select "Relay 1-IR Corporate Main Entrance Reader".
 - b) Select **Energize Relay** as the override command.
 - c) The duration is for 5 seconds.
 - d) Click **Save and Close**.
- 6 The last action item is to turn the LED Green on the Reader attached to the door.
- a) Select the reader attached to the door that provides access to the Area as the device. In this example, select "Proximity - IR Corporate Main Entrance".
 - b) Next select **LED Green** as the command.
 - c) The duration is for 5 seconds.
 - d) Click **Save and Close**.
- 7 In this example we want to lock all the corporate offices at the same time. In order to do this you need to define Override Tasks for all the devices attached to the entry doors of these buildings. Follow the same steps described above. Once you have defined all the tasks you can attach them to the Override Set we created earlier. Executing this Override Set locks all the entry doors of buildings included in this Set.

Reset momentary lock

Next you need to define the tasks and actions that will reset these devices to their initial state.

- 1 First define an **Override Set** E.G. "Reset Momentary Lock".
- 2 Define an **Override Task** called Reset Momentary Lock - IR Corporate Main Entrance.
- 3 Then define the actions. First you need to reset the contacts. Select the contact that you shunt in the previous step as the device. For this example select IR Corporate Main Entrance DOD. Now select the override command **Contact Reset (all)**.
- 4 Next, you need to reset the relay. Select the relay and select the command **Relay Reset**.
- 5 Then reset the LED. Select the reader and choose the command **LED Reset**.

Executing this Override Task will reset all the devices (Contacts, relay and reader) attached to the "IR Corporate Main Entrance" to their initial state. Like this you need to define Override tasks for all the devices attached to the doors you want to include in the above Override Set.

Lock forever

Follow these steps to define the Manual Override that will cause locking down of the doors for a longer period of time.

- 1 First define the **Manual Override Set**. Click the + sign under the Manual Override Set section to open the **Manual Override Set definition** window.

- 2 Enter a name for the set and noted pertinent to it. For this example we will use "Lock Down All Corporate Offices".
- 3 The next step is defining the Override Tasks that are included in this Set. Let us create a Task called "Lock Proximity - HQ Main Entrance". Enter the notes. Select the reader that is attached to the door you want to lock. Here it will be "Proximity - HQ Main Entrance".
- 4 Now you need to define the actions for this task. Open the Manual Override Action Definition window. The first action is to enable contact reporting. Select the contact (E.G HQ Main Entrance - DOD) and **Contact Reporting Enabled** as the Override Command. Leave the duration as zero (0) which means forever. Now opening this door will cause alarm until this contact is reset to its initial state. Click **Save and New**.
- 5 The next action is to enable the contact trigger. Select the same contact that you selected in the previous step and select the command **Contact Trigger Enabled**. Leave the duration as zero (0) which means forever. Click **Save and New**.
- 6 Now, select the relay as the device. (E.G Relay Two - Proximity Reader - HQ Main Entrance). Select the command **Release Relay**. The duration must be set to zero (0) to lock the door forever (until another action overrides this action).
- 7 The last action is to turn the LED Red. Select the reader and choose the command **LED Red**. E.G. "Proximity Reader - HQ Main Entrance." Set the duration to zero (0).

Reset lock

Follow these steps to reset the lock to its waiting state.

- 1 Define the **Override Set** called "Reset Lock - All Corporate Offices".
- 2 Then define **Override Tasks** that are going to include in this Set. Define an Override Task called "Reset Lock - HQ Main Entrance".
- 3 Then define the actions. First you need to reset the contacts. Select the contact that you shunt in the Lock Forever section as the device. For this example select "HQ Main Entrance - DOD". Now select the override command Contact Reset (all).
- 4 Next, you need to reset the relay. Select the relay and select the command **Relay Reset**.
- 5 Then reset the LED. Select the reader and choose the command **LED Reset**.
- 6 Executing this Override Task will reset all the devices (Contacts, relay and reader) attached to the "HQ Main Entrance" to their initial state.

View tab displays

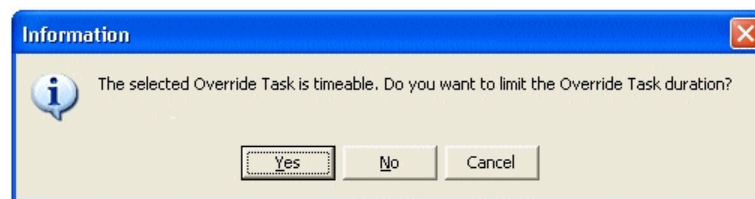
- 1 **Controller Tree View** – Navigate through physical connections to locate Overrides by device. Select the override and click **Execute Override Task** button located at the bottom of the window.
- 2 **Override Set View** – This is the default tab. Highlight a Set or Task to execute it, both buttons are available here. (**Execute Override Task** and **Execute Override Set**)
- 3 **Area Set View** - Navigate through Areas to select overrides defined for devices in an Area. Override Sets are not available in this tab.
- 4 **Reader, Contact and Relay Views** - The devices included in the currently defined Overrides are displayed. The Device ID (#), device name and Area information is provided. Individual Tasks may be executed under these tabs.

Note: The permissions granted to individual operators determine what will be available for display and execution in any of these views. Please refer to the System Security chapter for details.

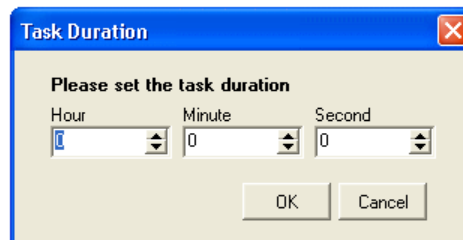
Timed Override Task and Set

Users can set a time duration for Manual Override Tasks if the Override Actions only affect a contact. In order for this option to be available, the Override Action duration must be set to zero. This feature is most useful for shunting reporting of transactions and alarms at certain contact points using an MRO for a specified duration of time. Previously, contact reporting could only be shunted via MROs indefinitely, and would have to be re-enabled later using another MRO.

When a timed Override Task is executed an information message pops up:



- Clicking **Cancel** causes the override to not be executed.
- Clicking on **No** leaves the override set to a duration of zero (executed forever).
- Clicking on **Yes** opens the Task Duration window.



Specify the length of time that the Override Task will run. Maximum duration of override is 18 hours, 12 minutes and 15 seconds. Clicking **OK** will execute the Override Task for the duration specified. At the end of the specified duration, the Override Task will stop and the device will return to its previous state. Clicking Cancel will default the Override Task to zero (executed forever).

Note: Users cannot set Task Duration for Override Tasks included in the Manual Override Templates available in the system.

Users can set Task Duration for Override Sets too. If all the Override Actions in every Override Task in the selected Override Set are set to only affect a contact and the durations are set at zero, then users can set Task Duration for the whole Override Set. When such an Override Set is executed, an information message is displayed prompting users to confirm the action (see the Information message showed above). Follow the same steps as you did for setting a Timed Override Task.

Automatic Override Definition

CHAPTER 28

Introduction

In certain circumstances it will be necessary for you to override a device's defined function on a regular schedule, such as unlocking a main lobby door during normal business hours. The Automatic Override module provides the means to do this. The normal function or state of a device is initially programmed into the device's database through the System Manager module. The **Schlage SMS** will automatically execute an Automatic Override to affect a change in a device's normal state.

For instance, if you want to unlock the main lobby doors at 8:00 AM and relock these doors at 6:00PM, you would program an Automatic Override on the Reader that controls that door and assign a Time zone with the interval hours of 8:00AM to 6:00PM. Another useful feature is that an Automatic Holiday override, for example, New Years Day 2004, can also be associated with the override device to prevent the doors from unlocking when the business is temporarily closed. This is possible because in the System Manager a Holiday is attached to a Holiday Set.

In turn, Holiday Sets are defined for each device. Once an Automatic Override has been defined, no further human intervention will be necessary for executing the task.

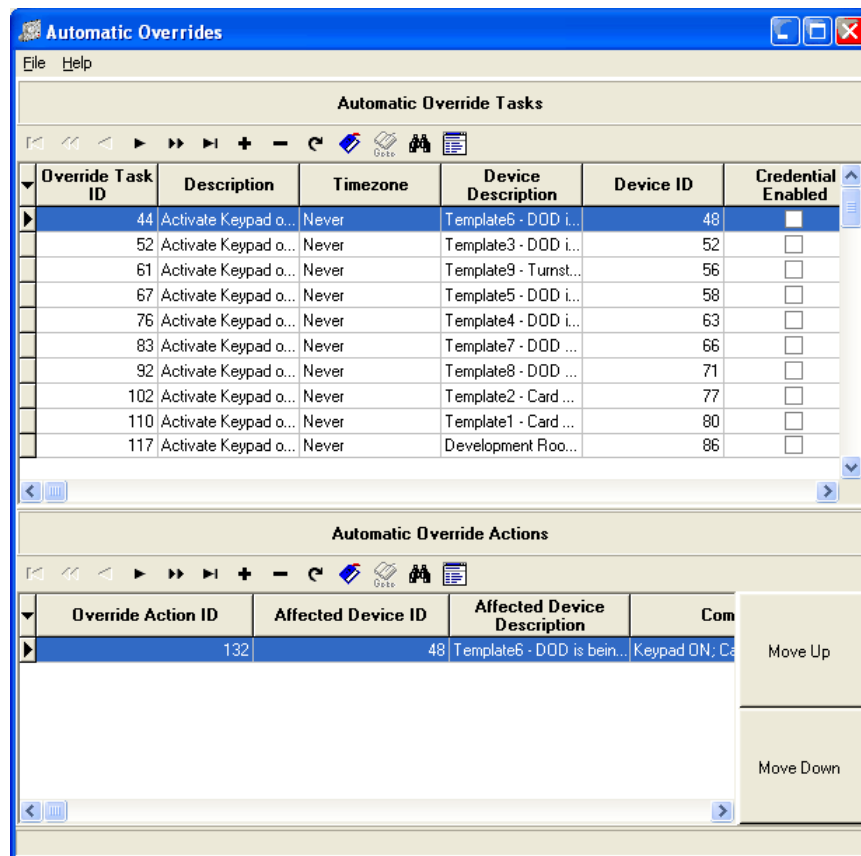
Accessing the application

- 1 Open the **System Launcher** by double clicking the **Launcher** icon on your desktop or select **Start>Programs>SchlageSMS>SchlageSMS**.
- 2 The login window, opens. Enter your user id and password.
- 3 In the **System Launcher** window, double click on **Automatic Override Definition** icon.

Working with Automatic Overrides

Overview

The main screen of the **Automatic Override Definition** is divided into two sections; Automatic Override Tasks and Actions. Both grids contain a Navigation/Tool Bar through which all functions are performed.



Programming Automatic Overrides

The Automatic Overrides consists of Override tasks and Actions. The programming of Automatic Overrides is very similar to Manual Overrides. In Automatic Overrides you need to select a time zone. The override task will be executed automatically at the time zone specified here.

Define Automatic Override Tasks

- 1 The Task must be created first. Click on the + icon in the upper tool bar to open the **Automatic Override Task Definition** window.

The screenshot shows the 'Automatic Override Task Definition' dialog box. It has a blue title bar with a close button. Below the title bar is a menu bar with 'File', 'Search', and 'Help'. The main area contains several sections:

- * Description:** A text field containing 'Auto Unlock Lobby Door'.
- Notes:** A large, empty text area with a vertical scrollbar.
- * Associated Device:** A text field containing 'Lobby Reader' and a green expand button (three dots).
- Timezone:** A text field containing 'Weekdays' and a green expand button (three dots).
- Credential Enable:** An unchecked checkbox.
- Attach a pair of Suspend and Restore manual Overrides:** A checked checkbox.

 At the bottom of the dialog are three buttons: a help icon (?), 'Save and Close', 'Save and New', and 'Close' (with a red X icon).

- a) **Description** - Choose a name for the type of Override you are creating. Maximum characters allowed for Description field is 64.
- b) **Notes** - Enter the details about the Override.

Note: You may have to create a specialized Time zone in **System Manager** first, depending on your needs.

- c) **Associated Device** - Click the expand button to open the Device Selection window. Select the device of which you need to override the normal state.
 - d) This screen contains five tabs through which you can select the Device(s) to be affected: Controller and Area Tree, Readers, Relays and Contacts. The Reader tab is the default tab in this window.
 - e) **Readers, Relays, Contacts, Offline Locks** - Each of these tabs display all the defined devices of each type in your database.
- 2 **Time zone** - Click inside this field or on the expand icon to open the **Select a Time zone** window. A list of defined time zones is displayed. Highlight your choice and click **OK**.
 - 3 **Credential Enable** - If this field is enabled, to trigger the automatic override a valid credential must be presented at the associated device.
 - 4 **Attach a pair of Suspend and Restore Manual Overrides** - Select this option to temporarily change the device status and restore it to the normal ARO state. A sample scenario would be:

The front door is unlocked from 8am to 5pm, Monday through Friday. The receptionist may want to lock the door when he/she leaves for lunch and then put it back on the ARO schedule on her return from lunch. In that case, he/she can suspend the ARO and restore the device to its normal state by sending a pair of MROs. The required MROs (Suspend Automatic Override and Restore Automatic Override) are created automatically in the **Manual Override Definition** (see "Programming Manual Overrides" on page 354) program when an ARO is created with the Suspend and Restore option enabled.

Note: The Suspend/Restore function will only work with firmware version 5.86. If an older version of the firmware is in use the Suspend function will replace the Reset function and the Restore function will be disabled.

- 5 Click **Save and Close**. After all fields have been entered, you should see the Override Task listed on the upper half section of the main screen. The feature works only with firmware version v5.72.

Note: An ARO defined for an offline lock does not require ARO actions. The actions are disabled for an offline lock device.

Automatic Override Actions

The Override Task must be associated with an Override Action.

- 1 Highlight the Task and click the + icon in the tool bar of **Automatic Override Actions** to open the **Automatic Override Action Definition** window. Use the expand button or click the field to make your entries.
 - a) **Device Action Affects** - This option opens the Reader, Relay, and Contact Selection window. Make your selections the same as described earlier for this window.
 - b) **Override Command** - This option opens the **Select an Override Command** window that displays a list of the commands that are associated with the Device type chosen previously. These commands are simply the function you want the Device to perform upon execution of the Override.

Note: You must update the reader controller's for the **Automatic Override** to take effect with dial-up boards.

Example for an Automatic Override

The following is an example for defining an automatic override.

- 1 Open the **Automatic Override Task Definition** window. Enter the description and notes pertinent to it. For this example we are going to define the steps required for unlocking a door at 7.30 AM to 5.00 PM automatically. Enter the description "Unlock Proximity Reader - HQ Main Entrance". Select the timezone corresponding to it. (You need to have a pre-defined time zone). In the **Associated Device** field select the reader attached to the door which you want to unlock automatically. Select the Credential Enable check box. If this option is enabled a valid credential access is required to trigger the readers scheduled to unlock during a scheduled period. Click **Save and Close**.
- 2 Now you need to define the actions that will cause the door to open at the specific period of time.
 - a) The first action is to disable contact reporting. Select the DOD contact that is attached to the door. as the **Device that Action Affects**. E.G. DOD 1- HQ Main Entrance. Choose **Contact Reporting Disabled** as the command. Click **Save and New**.
 - b) Next action is to disable contact trigger. Select the same DOD you chose in the previous step. Select **Contact Trigger Disabled** as the Override Command. Click **Save and New**.
 - c) Next choose the relay as the device. E.G. "Relay 1- HQ Main Entrance". Select **Energize Relay** as the command. Click **Save and New**.

- d) The final action is to turn the LED green. Select the reader attached to the door as the device. E.G. "Proximity Reader - HQ Main Entrance." Select **LED Green as** the command. Click **Save and Close**.

Auto unlock Offline Locks

The system allows the user to define actions for automatically unlocking an off-line lock. A maximum of sixteen (16) ARO definitions are allowed per offline lock.

Follow these instructions to unlock an offline lock.

- 1 Open the **Automatic Override Task Definitions** window.
- 2 Add a description and notes for the action.
- 3 Select an Off-line Lock as the associated device.
- 4 Select a timezone. The system allows users to attach timezones with two intervals, only if that is a spanning midnight timezone. The first interval should end at 11.59.59 PM, and the second interval must start at 12.00.00 AM
- 5 Select the **Credential Enable** check box. If this option is enabled a valid credential access is required to trigger the readers/ offline locks scheduled to unlock during a scheduled period.
- 6 For example, a reader in a lobby is programmed to unlock at 9:00am Monday through Friday. Each day after 9:00am, the reader will await a valid access grant from an authorized cardholder before setting the mode to unlocked.
- 7 Click **Save and Close**.

Note: Since there is only one action (unlock), an ARO action for Offline Lock does not require any tasks attached to it.

Navigation/Tool bar options

- 1 **Navigation arrows and bookmark buttons** - standard for locating and marking records
- 2 **Add/Delete** - functions may only be performed using these buttons in both sections
- 3 **Refresh** – will restore the contents of the data set after filtering
- 4 **Filter** – only found in the Tasks tool bar, used for normal filtering of displayed information.
- 5 **Search** – This feature allows specific conditions and values to be entered to locate records.
- 6 **Edit** – opens the currently selected record for modification.

Search

- 1 Open the generic search dialogue by clicking on the binoculars.
- 2 Enter the search word in the search criteria field and click **Find Now**.
- 3 The program searches all the records containing the search word or letter.

Advanced Find

Using Advanced Find, you can build the search criteria by selecting appropriate entries from the drop down list box and entering specific value in the value field. You have to select a specific field name, condition and a specific search value.

Advanced Find feature uses Boolean logic to create complex and highly precise searches. Boolean logic uses three connecting operators (NOT, AND OR) to narrow or broaden a search or exclude a term from the search. It is the process of linking criteria to narrow or expand a search through the use of **NOT**, **AND** or **OR**.

The Advanced Find feature helps the operator to customize the search function. Operators can define the searches and save them for a later use. The saved search criterion is displayed only for the operator who defined it.

- 1 Click on the **Advanced Find** tab located on the top of the Search window.

- 2 The **Advanced Find** window opens. Define your search criteria.

For example, if you want to search for Override Task ID = 55, you need first select the left parenthesis from the list box.

Parenthesis can be used to create nested search clauses. Using the parenthesis one can override the standard order of priority (left to right) for each Boolean statement in the search.

- 3 Select Override Task ID as the Field Name.

- 4 Select equal to (=) as the condition.

- 5 Enter the value as 55.

- 6 Provide the closing parenthesis at the end.

- 7 If you want to specify additional search condition you can select AND/OR from the list box.

E.g. If you want to search for Override Task IDs less than or equal to 55 and Description containing the word "exit" and Override Task IDs greater than or equal to 55 and Description containing the word "suppress", define the search criteria as follows.

((Override Task ID>= 55) AND (Description LIKE%exit%)) OR ((Override Task ID<= 55) AND (Description LIKE%suppress%))

When you run the search you will get results with Override Task IDs less than or equal to 55 and with the word "exit" or Override Task IDs greater than or equal to 55 with the word "suppress".

- 8 When you are satisfied with the criterion, click **Add to List** button. If the criterion is not valid, it is displayed in red under the Where Clause section. When the criteria becomes valid the font color changes to black.

- 9 Once you have defined the criteria click **File>Save**.

- 10 Add a description to your search and click **OK**.

- 11 The new search will be saved and listed under the **Advanced Find** button.

Universal Triggers

CHAPTER 29

Introduction

The Universal Trigger module enables an action or a series of actions in response to a trigger event that is sent across *any* or *all* the CIMs, controllers, readers, contacts or relays throughout the system. A trigger, for example activating a specific contact, initiates the actions. Events must be pre programmed in the **Manual Override Definition** module and associate with an **Override Task Set**. These events are then associated with a device, transaction, time zone, and override task set in the **Universal Trigger** module.

To designate a universal trigger, determine what event should happen, such as opening all emergency exit doors from outside so that the fire department has free access. Then you determine what “trigger” will cause a command to be sent system wide to achieve the desired event. The software constantly scans for these trigger events and once found, instructions are sent system wide and the doors are opened automatically.

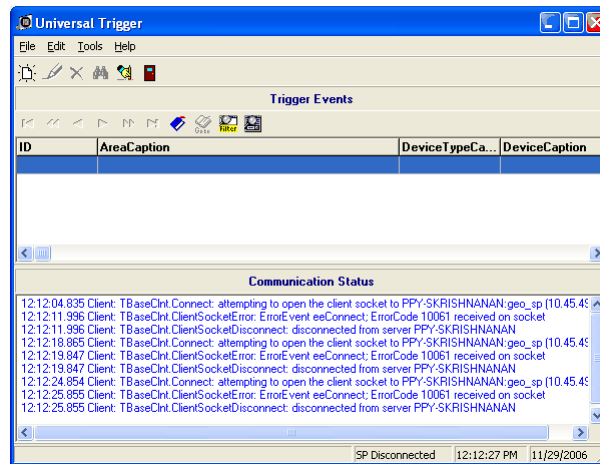
Therefore depending on your company needs, with minimum of effort such as a flick of a switch or a push of a button, almost immediately, doors will be unlocked, placed in a lockdown state or emergency lighting can be switched on. Any programmed override task set can be designated as a **Universal Trigger**.

Accessing the application

- 1 Open the **Schlage SMS** software by double clicking on the launcher icon on your desktop or select **Start>Programs>Schlage SMS>Schlage SMS**.
- 2 Enter your assigned user ID and password.
- 3 In the System Launcher window, double click on **Universal Triggers** icon.

Overview

Options are accessed using Menu bar and Toolbar shortcuts. The Trigger Events grid displays triggers that have been programmed. The fields are Trigger ID, Area, Device Type, Device, Transaction Code, and Override Set. The communication information is viewed under the status window.



Manual Overrides and Trigger Events

The Manual Overrides that are associated with any universal trigger event must be programmed (prior to all event triggers) in the **Manual Override Definition** module and assigned to an Override Set. In turn, these override sets are associated with an event in the Universal Trigger module. It is very important to understand that areas, time zones, and devices in the **Hardware Map** of **System Manager** must be defined properly.

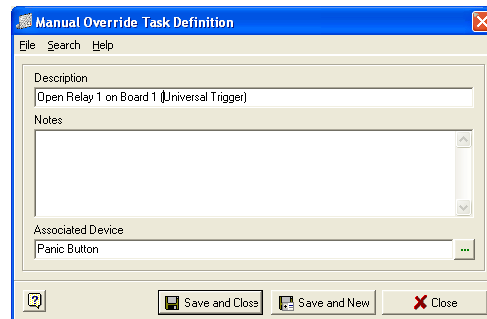
The example used in this chapter is to program universal triggers that will unlock emergency fire exit doors. Without valid access, these doors would normally be locked, such as outside perimeter doors to a building.

By energizing the relays for these doors, the fire department will have free access into and out of the building.

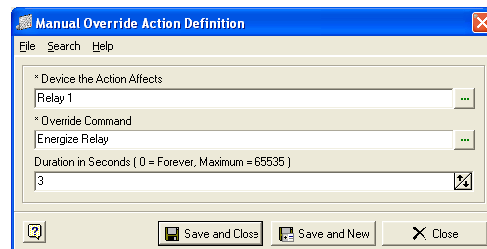
To program a trigger, you must determine two criteria.

- 1 Specify the incident (s) that must happen. An input will open relays on specific boards throughout the system. Make a note of each board that will be affected. For example, this input will open relays 1 & 2 on Controller Board One and relays 1 & 2 on Controller Board two.
- 2 Specify the trigger to use to cause the desired result to happen. Such as a contact active on input one of controller one will be the trigger in the system to cause programmed relays to energize.
- 3 Once your conditions have been determined then the Override Set, Tasks and Actions must be programmed in the **Manual Override Definition** module. We are using "Open all Fire Exits" as an example.
- 4 In **Manual Override Definition** create an **Override Set** that is quickly identified as a universal trigger that opens emergency exits.

- 5 In the **All Override Tasks** tab, define a task for each action that will be part of the universal trigger. The **Associated Device** is the hardware that will control the trigger. In our example we have used **Panic Button** (Contact 1 on Direct Board 1.)
- 6 The **Schlage SMS** software constantly scans for triggers. When the Panic Button is pushed (Contact 1 on Board 1) then a command is sent system wide to energize the relays that have been programmed in this override. Drag the **Override Task** and drop it into the Override Set.

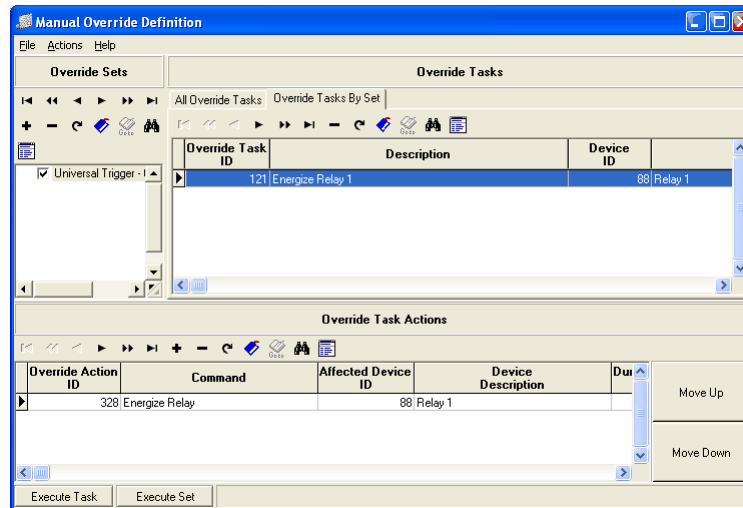


- 7 For each Override Task we must assign Task Actions. In this example we will only program Relay 1 and Relay 2 on Controller board 1 to energize when Contact 1 on Controller 1 becomes active. You may add as many devices as is necessary to accomplish your task.
- 8 An on / off switch or button can be wired to the controller board that will cause the contact active transaction.



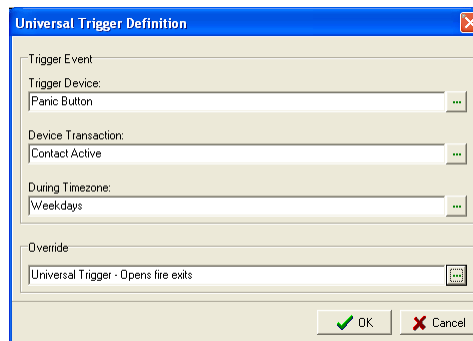
- 9 We also want Relay 2 on Board 1 to be energized during this trigger. Program this task as well. Once you have defined the override actions, the next step is to define the Override Task for board 2 that are also associated with this Trigger Event. Follow the same format that you used for board 1. This Override Task must also be dragged and dropped into the universal trigger Override Set.

- 10 Program the relay actions on Board 2. After you have completely defined all tasks and task actions for the Override Set, verify that they appear in the Override Tasks By Set tab. To test your programming use the **Execute Task** or **Execute Set** button on the bottom, left of the window.



Programming a Trigger Event

- 1 In the **Universal Trigger** module, select **Edit>New** to open the Universal Trigger Definition form.



- a) **Trigger Device** - This is the specified device that will cause commands to be sent system wide.
 - b) **Device Transaction** - This is the device action that initiates the trigger.
 - c) **Timezone** - The time frame that this trigger will be active.
 - d) **Override** - This is the Override Set that has been defined in **Manual Override Definition**.
- 2 In the example above, a Panic button (contact) will automatically trigger commands to open all fire exits without human intervention.

Menu options

File

- 1 **Verbose** - When checked, a toggle option allows for more detailed messages in the Communication Status display.
- 2 **Exit** - This option closes the Universal Trigger module.







Edit

- 1 **New** - Adds a new Trigger Event
- 2 **Modify** - Allows editing of a currently highlighted Trigger Event
- 3 **Delete** - Removes the currently highlighted Trigger Event

Tools

- 1 **Status Bar** - Toggles the status bar on and off.
- 2 **Tool Bar** - Displays or hides the Tool Bar.
- 3 **Clear Status Display** - Clears messages in the Communication Status window.

Toolbar options

- 1  New - Use this icon to open our Universal Trigger Definition form and create a new Trigger Event.
- 2  Browse - Click the Browse button to select the Trigger Device, Transaction, Time zone and Override Set.
- 3  Edit - This option is used to modify a Trigger Event.
- 4  Delete - Eliminates the currently highlighted Trigger Event
- 5  Clear Status Display - Removes all messages in the Communication Status window.
- 6  Exit - Closes the Universal Triggers module.

Elevator Control

CHAPTER 30

Introduction

The Schlage SMS offers a comprehensive and economical way of controlling the building's elevator units. Essentially, it is an integrated system of specific Controllers, Areas, Relays, Contact points and Readers, which are defined in the System Manager Module.

Elevator Control Setup

For successful operation of the elevators, you must accurately define the following: **Areas, Controllers, Contact Points, Readers and Relays**. As well, all the cardholders who use the elevators must have their area access defined. This was naturally done at an earlier stage. Below is an outline of the fields that require definition when setting up your elevators.

Define Areas

Areas are very important while setting up the elevator control. Each floor must be defined as an Area in the system and relays and contacts must be attached to these Areas.

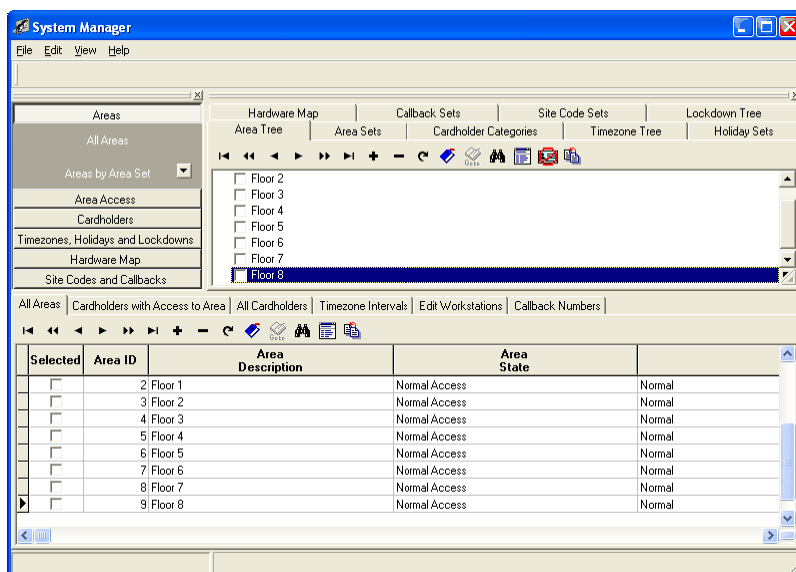
According to the reader type if there are 38 floors in a building each floor (Location Or Area) must be attached to one relay and one contact point.

If the reader type is **Elevator Reader - (Enable all Floors)** (for further information on these reader models see the section **Reader Types and Security Issues** in this chapter) each floor only needs to attach to one relay, but if the reader type is **Elevator Reader - (Scan Call Buttons)** each floor must have a relay and contact point defined with same Area Access.

Also the cardholder must have access to each of these areas to get a valid access transaction. If the reader type is **Enable all Floors**, when a cardholder swipes the card, all the relays attached to the floors to which the user has access are activated. When the cardholder presses the floor selection button all the activated relays are released and the elevator travels to the selected floor. If the reader type is a **Scan Call Button**, when a cardholder swipes the card and presses the call button the relay attached to that particular floor (Location or Area) is activated and the cardholder is given access to the floor. Follow these directions to define an Area for the Elevator Control.

Note: For this example we have defined 38 floors and 3 elevators. Low Rise Security Elevator travels from 1 to 17 floors, High Rise Security Elevator covers 18 to 38 floors and the Freight elevator travels from 1 to 38 floors. So we need four SIONX 24 boards. The first SIONX 24 board with 24 relays covers 1-17 floors and the second one would cover floors 18-38. Also the parent SRCNX board is placed in the computer room and the child SRCNX is located in the elevator equipment room. (See the hardware diagram). The Elevator Control functionality can be deployed to a building that has any number of floors and any number of elevators.

- 1 Open the **System Manager** Program.
- 2 Click on the Area Tree button to open the Area Tree section. Click on the + sign to open the **Add Area** Wizard. For example if there are 38 floors in your building, define each floor as an Area.



Define Controllers

The next step is defining controllers. Schlage Security Management System uses SIONX 24 boards for securing elevators. You need to attach these boards to a SRCNX Child board located in the elevator equipment room through an RS 485 connection. A Parent SRCNX is connected to the PC via RS 232 protocol. (See the diagram in the Hardware Set up section).

Note: In Elevator Control, the SRCNX - SIONX 24 configuration can be a direct or a parent-child configuration depending on your company's requirements. The communication can be through direct, IP or dial-up connections.

- 1 In the **System Manager** program click Hardware Map tab on the tab window. Then click on **Edit Controllers**.
- 2 On the grid window click on the + sign to add the parent **SRCNX (master SRCNX)**.
- 3 On the **Controller Definition** window, enter the descriptions for the Parent SRCNX board (master SRCNX).

Controller Definition

File Search Help

* Description
Parent SRCNX

Notes

* Attached To I/O Port or Master
CIM Port 1

* Location
Off Site

Controller Model
SRCNX-16

Site Code Set
No defined site codes

Holiday Set
No defined holidays

* Locale Timezone
(GMT-05:00) Eastern Time (US & Canada)

IP Address or Host Name
IP Port Number
3001

Phone Number
Master Channel
N/A

Board Address
N/A

Schedule Timezone
Never

Network Device Type

Administrative Level Password
Access Level Password

☒ Installed
☐ Reinstall All Devices

Save and Close Save and New Close

- 4 Next, define the child SRCNX board and attach it to the Parent SRCNX (master SRCNX).

The SIONX 24 Board and Floor Assignment

Each SIONX board has twenty four relays and contact points. Each floor must be associated with a unique relay and a contact. This would mean that Relay 1 is designated for Floor 1, Relay 2 is for Floor 2, and so on. The relay and floor assignment need not be in this order. They can be assigned in any order that is suitable for your company's requirements.

Note: A maximum of four SIONX 24 boards can be attached to a SRCNX board, which will control a maximum of ninety (98) floors.

If you have a building with 24 or less floors, you only need to have one SIONX 24 board. The SIONX 24 board can support any number of elevators provided the total number of floors serviced by all the elevators does not exceed twenty four.

When you implement a freight elevator which travels from 1-38 floors we need to have two more SIONX 24 boards to cover all the 38 floors.

Follow these directions to define the SIONX24 controllers.

- 1 Click on the + sign on the grid window selecting the tab **Edit Controllers**.
- 2 Define four SIONX 24 boards one by one (to cover 38 floors including freight elevator) and attach each of them to the Child SRCNX board.

An example of the controller definition is given below.

- 3 Define SIONX 24 boards for Low Rise, High Rise and Freight Elevators. In the example given, the relays on this board would control the Low Rise Elevator.
- 4 Select SIONX 24 as the controller model.

Define Readers

Next you need to define three readers for three elevators.

Requirements for Elevator Reader

- Schlage SMS 5.57 (SRCNX) firmware with 5.06 software (allows only one elevator reader)
- Schlage SMS 5.64 (SRCNX) firmware with 5.09 software and above (allows multiple readers)

Note: In elevator control there are only four readers allowed per controller.

- 1 Click on **Edit Readers** tab on the Tab window. On the Grid window the **Edit Readers** tab is active and click on the + sign to define the readers.

- 2 Define one reader for each elevator and attach them to the Child SRCNX board.

The screenshot shows the 'Reader Definition' dialog box. The 'Description' field is filled with 'Low Rise Security Elevator'. The 'Notes' field is empty. The '* Attached To' dropdown is set to 'Child SRCNX'. The '* Provides Access To Area' dropdown is set to 'Floor 1'. The '* Reader Model' dropdown is set to 'SRINX - 1 RELAY'. The '* Reader Type' dropdown is set to 'Elevator Reader (Scan Call Buttons)'. The '* Door Type' dropdown is set to 'Pedestrian'. The 'Antipassback Time (Minutes)' is 0, 'Channel Number' is 1, and 'Reader Address' is 1. The 'Reader Template' dropdown is set to 'Template2 - Card Reader for Entry and REX for Exit (No DOD)'. The 'Keypad Reader' checkbox is unchecked, 'Guest Sign In Reader' is unchecked, 'Installed' is checked, 'Reinstall All Devices' is unchecked, 'Degraded Mode' is checked, 'Guest Sign Out Reader' is unchecked, and 'Auto Relock' is unchecked. The bottom buttons are 'Save and Close', 'Save and New', and 'Close'.

- 3 **Description and Notes** - Enter an identifiable description for the reader. For this example we will use Low-Rise Security Elevator as we are defining this reader for the Low rise elevator. In the Notes field enter the floors that the elevator covers.
- 4 **Attached to** - This delineates which board the reader is attached to, thus providing access to those areas covered under the board. For this example select Child SRCNX as the controller board.
- 5 **Provide Access to Area** - For an elevator reader the access to an area is **OFF SITE**. Readers in the elevator control cab provide access to multiple Areas. In elevator control it is the relay that is attached to an Area that determines the Area access.
- 6 **Reader Model** - This depends on which model you have purchased but is almost always a SRINX.

- 7 **Reader Type** - This determines the type of access. Since you designate this reader for your elevator, you must select either the Elevator Reader (Scan Call Button) or Elevator Reader (Enable All Floors) definition. Your selection depends on your security needs. (And if you have the elevator configured for the extra wiring to scan the call button). In the screen capture below shows the definition for a **Scan Call Button** reader.

Reader Definition

File Edit Search Help

* Description
Freight Elevator

Notes

* Attached To
Child SRCNX

* Provides Access To Area
Off Site

* Reader Model
SRINX - 1 RELAY

* Reader Type
Elevator Reader (Scan Call Buttons)

* Door Type
Pedestrian

Antipassback Time (Minutes) Channel Number Reader Address
0 3 1

Reader Template
Template2 - Card Reader for Entry and REX for Exit (No DOD)

☐ Keypad Reader ☒ Degraded Mode ☐ Auto Relock
☐ Guest Sign In Reader ☐ Guest Sign Out Reader
☒ Installed
☐ Reinstall All Devices

Save and Close Save and New Close

- 8 **Door Type** - The standard type is Pedestrian.
- 9 **Keypad Reader** - Select this check box if you are using a keypad reader.
- 10 **Degraded Mode** - The degraded mode does not apply to elevator readers. For more information on Degraded Mode refer to System Manager Chapter (Reader Definitions).

Reader Types and Tracking Issues

Elevator Control has two types of readers while each one is designed to handle routine elevator usage, you can specify more or less security by your choice of reader. The two reader types are **Enable All Floors** and **Scan Call Button**.

Enable All Floors

Key Features:

- **Cardholder's Area Access Privileges determines the relay**

When the cardholder swipes the card, all the relays for the appropriate floors are activated.

Selecting the button closes the call and its corresponding relay thus directing the elevator to the floor represented by the closed relay.

Because all of the appropriate relays are energized, there is no monitoring of which floor is chosen. Thus security is low. In essence, **Enable All Floors** simply determines access to the cardholder. For example, Cardholder John Smith has access to Floor 1, Floor 2, Floor 3, Floor 4 and Floor 5. When the cardholder presents the card in the reader located in the Freight Security Elevator, relays 1, 2, 3, 4 and 5 are simultaneously energized. When Smith presses the floor selection button for Floor 4, he closes the call and Relay 4, which then makes the elevator proceed to Floor 4.

The screenshot shows the 'Transaction Monitor - Connected - Parsippany NJ' window. It contains two main transaction logs. The top log, 'Cardholder Transactions', shows a single entry for a 'Valid Access' by John Smith at 14:10:49. The bottom log, 'Device and Operator Transactions', shows a sequence of events: five 'Relay Released' events for relays 5 through 1 on floors 5 through 1, followed by five 'Relay Energized' events for the same relays. Each entry includes a timestamp, transaction type, device ID, area, and controller ID.

Transaction Date	Transaction	Cardholder	Encoded ID	Device	Controller
07/22/2003 14:10:49	Valid Access	21970: Smith, John	11099	2400: Freight Security Elevator	130: CHILD GRCHX

Transaction Date	Transaction	Device	Area	Controller
07/22/2003 14:10:54	Relay Released	2400: Relay 5	403: Floor 5	130: CHILD GRCHX
07/22/2003 14:10:54	Relay Released	2438: Relay 4	752: Floor 4	130: CHILD GRCHX
07/22/2003 14:10:54	Relay Released	2437: Relay 3	426: Floor 3	130: CHILD GRCHX
07/22/2003 14:10:54	Relay Released	2435: Relay 2	523: Floor 2	130: CHILD GRCHX
07/22/2003 14:10:54	Relay Released	2408: Relay 1	881: Floor 1	130: CHILD GRCHX
07/22/2003 14:10:49	Relay Energized	2400: Relay 5	403: Floor 5	130: CHILD GRCHX
07/22/2003 14:10:49	Relay Energized	2438: Relay 4	752: Floor 4	130: CHILD GRCHX
07/22/2003 14:10:49	Relay Energized	2437: Relay 3	426: Floor 3	130: CHILD GRCHX
07/22/2003 14:10:49	Relay Energized	2435: Relay 2	523: Floor 2	130: CHILD GRCHX
07/22/2003 14:10:49	Relay Energized	2408: Relay 1	881: Floor 1	130: CHILD GRCHX

The transaction monitor shows all the relays that are energized.

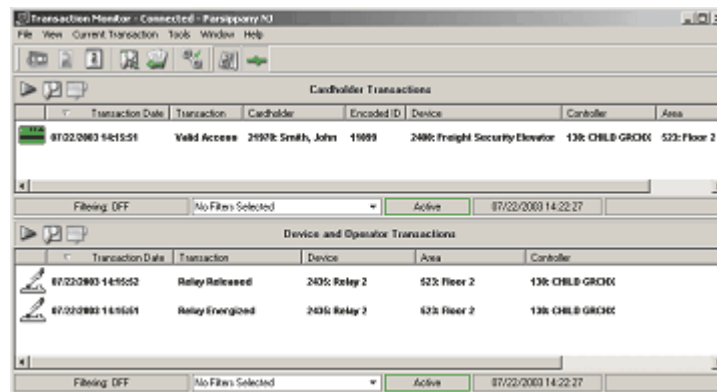
Scan Call Button

Key Features - After the card is swiped, the cardholder's choice of the floor (the call) activates the corresponding relay, thus closing that call and relay indicating which floor the elevator cab should go to.

Due to the fact that the input on the call button determines which relay is energized, the Transaction Monitor can track it and security is enhanced. This is unlike **Enable All Floors**, which entails the swipe of the card to energize all the floors (and thus relays) that the cardholder has access to. Still the transaction monitor shows valid or denied access transaction.

While the **Scan Call Button** allows the **Transaction Monitor** to monitor the cardholder access to the elevator, this is a more expensive option due to the need for extra wiring from the elevator cab to the SIONX 24.

The following example shows the transactions that occur while the cardholder John Smith using the Freight Security Elevator with the **Scan Call Button** reader. He has access to Floors 1 to 5. When he swipes the card no relay is activated. As soon as he presses the call button for Floor 2, the Transaction Monitor shows that relay 2 is energized.



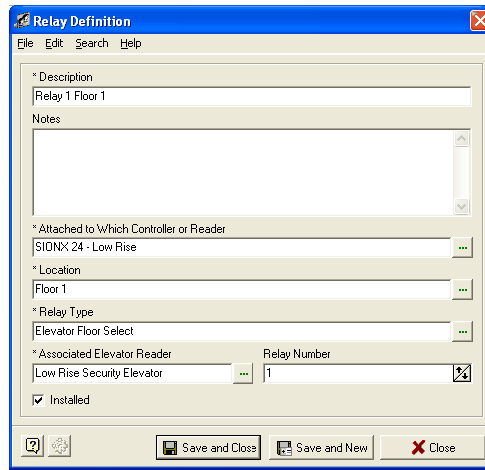
Only the relay attached to the floor selected is activated.

Define Relays

You need to define one relay for each floor. Here for this example we have 38 floors. So you need to define 38 relays.

- 1 Open the **Options Bar** and select **Hardware Map** and click **Edit Relays** (this automatically opens the corresponding hardware tab on the grid window to the right). On the bottom of the information grid, the Edit Relays tab is displayed.

- 2 Click on the + sign to open the **Relay Definition** window.



There are a variety of fields on this window, among which you should define the following:

- 3 **Description** - Type in the name of the respective Relay you are configuring, such as Relay 1 on Floor 1.
- 4 **Notes** - If necessary, write any pertinent information about this relay.
- 5 **Attached to Which Controller or Reader** - Define the controller or reader to which the relay is attached to, such as SIONX 24 LOW RISE.
- 6 **Location** - Select the location (area) of the Relay, such as Floor 1.
- 7 **Relay Type** - As this relay is used for an elevator, change this to *Elevator Floor Select*.
- 8 **Associated Elevator Reader** - Select the elevator reader to which this relay is attached.
- 9 **Relay Number** - Type in the number of the respective relay. It is good to be consistent and match Relay 1 with Floor 1 and so on.

Define Contacts

You need to define contacts only if you are using the reader as a *Scan Call Button*.

- 1 Select **Edit Contacts** under the Hardware Map on the Options Bar. This opens up the Edit Contacts tab on the information grid below.

- Click on the + sign on the Edit Contacts tab. This opens up the **Contact Definition** window. You have a variety of fields to define, most of which correspond to the **Relay Definition** window.

- Description** -Type in the name of the respective contact you are configuring, such as Contact 24.
- Notes** - If necessary, write any pertinent information about this contact.
- Attached to Which Controller or Reader** - Define the controller to which the contact is attached to, such as SIONX 24 FRIEGHT ELEVATOR 1-24.

Note: The above example shows the SIONX 24 which controls up to 1-24 floors.
- Location** - Select the location (area) of the contact, such as Floor 24.

Note: It is important that the location you select here should match with the location you selected for the corresponding relay to get a valid access.
- Contact Type** - Contact type must be **Elevator Call Button**.
- Associated Elevator Reader** - Select the elevator reader to which this contact is attached.
- Input Number** - Enter the input number for the contact. Use the up and down arrows to select the input number. Input 1 on SIONX 24 will be connected to elevator call button 1 and input 2 to call button 2 and so on. If there are 38 floors you need 38 inputs wired to 38 elevator call buttons.

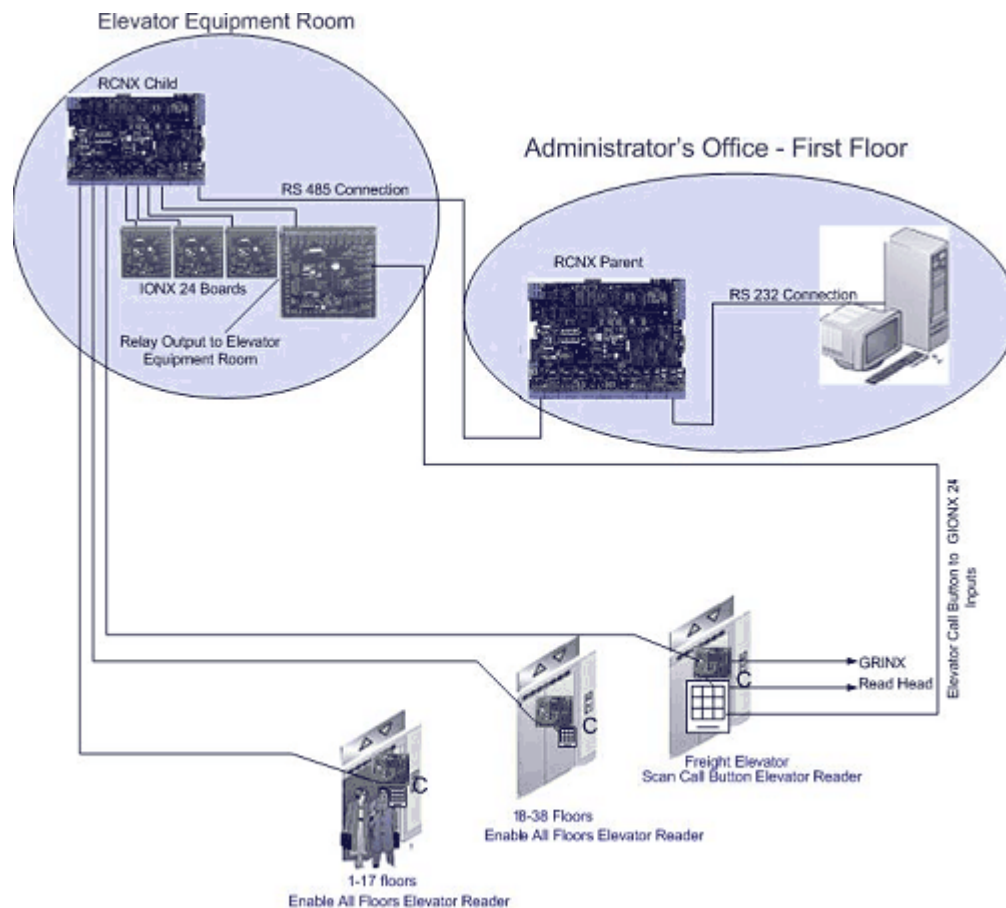
Invalid Transactions for Elevator Control

The following is the list of invalid elevator control transactions.

- Access Denied - Invalid site code
- Access Denied - Badge not in controller memory
- Access Denied - Invalid PIN entered
- Access Denied - Badge not yet activated
- Access Denied - Badge has expired
- Access Denied - Badge has been blocked from all access

- 7 Access Denied - Invalid Issue Code
- 8 Access Denied - Access to area not permitted

Hardware Connection Diagram

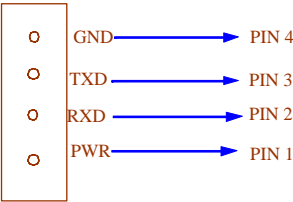


SIONX 24 wiring Instructions

- **K1 to K24 - Relays on SIONX 24 board**
 - Single pole double throw, mechanically latching relays rated at 30 VDC at 1 Amp
 - Inductive loads require noise suppression kit
 - Recommended cabling: 22 AWG/ twisted stranded pair
- **P 1 - P 12 - Contact Inputs**

Each SIONX 24 board has 24 contact inputs. For information on programming contacts refer to Chapter2 *System Manager*.

- **P 14 & P 13 - Power Source and Communication Wiring**
 - **P 14:** Power: 12 - 24 VDC



- **P 13:** 16 VAC to power the board, if it is not powered from the SRCNX.
- **SIONX 24 - SRCNX Connections (P14 to J4)**

SIONX 24 - P14		SRCNX - J4
Pin 1 (PWR)	To	Pin 1 PWR
Pin 2 (RXD)	To	Pin 2 RXDA
Pin 3 (TXD)	To	Pin 3 TXDB
Pin 4 (GND)	To	Pin 6 GND

The board can be powered from SRCNX through this connector.

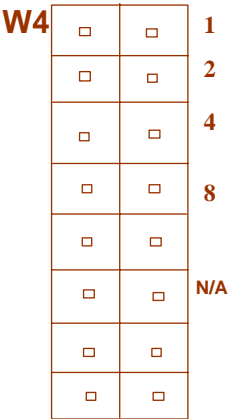
Be polarity conscious

Cable recommendations if powered from SRCNX: 4 -conductor, stranded, shielded.

Communication between SIONX 24 and SRCNX is via RS 485 protocol - 9600 baud rate.

Maximum distance between SIONX-24 and SRCNX is 4,000 feet.

- **W2 - SIONX 24 Addressing**



SIONX A	Addr.	Jumper Locations	SIONX B	Addr.	Jumper Locations
1		1 2 4 8	1		1 2 4 8
1		1 2 4 8	2		2 4 8
1		1 2 4 8	3		4 8
1		1 2 4 8	4		1 4 8
1		1 2 4 8	5		1 2 8
1		1 2 4 8	6		2 8
1		1 2 4 8	7		1 8
1		1 2 4 8	8		8
2		2 4 8	9		1 2 4
2		2 4 8	10		2 4
2		2 4 8	11		1 4
2		2 4 8	12		4
2		2 4 8	13		1 2
2		2 4 8	14		2
2		2 4 8	15		1
2		2 4 8	16		

- **SIONX 24 Addressing**
 - Jumpers 1,2,3 and 4: Multidrop addressing for the board
 - Jumper 5 and 6: No jumpers (Not used).
 - Jumper 7: No jumpers. (For future use)
 - Jumper 8: For diagnostic use only (No jumpers for normal use).
- **W6: RS485 line terminal**
- **S 1 - Reset**

To reset the board press the switch labeled as S 1.
- **W 4 & W 5**

With jumpers on the processor is in boot strap mode. No jumper for normal operation.

Report Scheduler

CHAPTER 31

Introduction

The **Report Scheduler** allows the user to automatically generate predefined reports on a scheduled basis. The Scheduler wizard guides you through the process of selecting a report from the Report Launcher module, creating a schedule and assigning a printer. Reports are scheduled to print on a daily or weekly basis at a specific time period. A schedule is created once and will automatically launch on the day of the week that is programmed. Any report that has been defined in the Report Launcher module can be assigned a schedule.

The **Report Launcher Schedule Service** must be installed and running in the Services program on a Window NT or Window 2000 machine that can connect to the Schlage SQL database. It is recommended that this service run on a server or on a very robust machine. Please refer to the page# 2 on chapter 1 for details on Report Scheduler Service. The **Report Scheduler Service Manager** allows the users to control the Service from the desk top. See page 3 for further details on this application.

Overview

The Report Scheduler module is where you create, edit and delete schedules. Make your selection using the tool bar icons or by selecting from the File menu. The grid window allows you to view important schedule information at a glance.

Report Scheduler Service

The Report Scheduler requires a service that runs on a Windows XP or Windows 2000 operating system that can connect to Schlage SQL database. However, the service may be either a Windows Service (non GUI version) or a **Schlage SMS** application that runs similar to the SP.

It constantly scans your database for a scheduled report that matches the current machine time (machine where the service is running). When it finds a match, the service sends the report to the defined printer or e-mail address without user intervention.

The GUI form of the Report Scheduler Service (ReportLauncherSvcApp.exe) can be added to the System Launcher (GUI version) and have the option of auto-starting like the SP when the system starts. It should not allow multiple copies to run on the same machine.

Note: Although this service can be run on multiple machines, it may cause adverse effects. If you have two copies of the Report Scheduler running on two different machines on the same system, you will get duplicate reports printed for each running Service. We highly recommend you to run this service only on a single machine where the system is running.

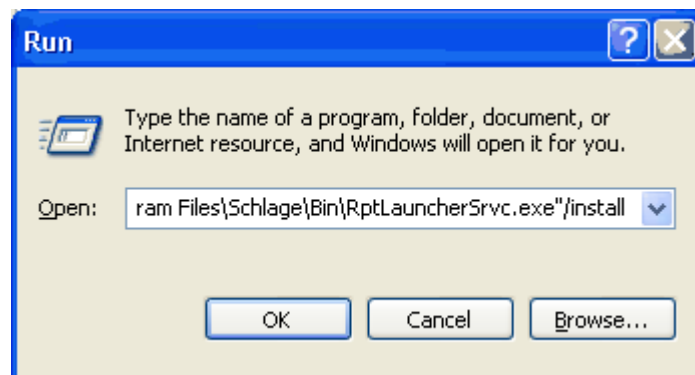
The non-Schlage version of the service is called RptLauncherSvc.exe. The RptLauncherSvc.exe file cannot be selected from the System Security program.

Setting up the service

Follow these steps to set up the non-GUI version of the Report Scheduler Service. This service can only be run on a Windows machine that supports services and can connect to the Schlage SQL database.

- 1 Run the executable on the machine with the following command line:

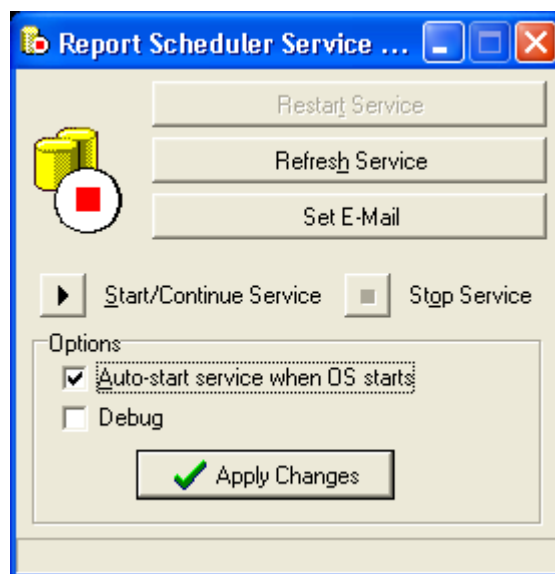
C:\Program Files\Schlage\Bin\RptLauncherSvc.exe/install (The path shown here may differ depending on the location of the executable)



Note: The Report Scheduler Service (non GUI version) requires a login that has sufficient privileges to *all* network resources necessary for printing reports. These network resources include the Crystal Reports (normally located in the Schlage\Data\Reports folder), the Network Printer where the report will be sent, and the Schlage Database. If the service login is set to "Local System Account" and the printer is on the network, the service login will not have sufficient privileges to access the network resource. "Local System Account" may only be used when the printer is on the same machine as the service. You may access the Log On settings through the Services application, by viewing the properties of the Report Launcher Service. The GUI version of the Report Launcher Service will use the login of the current windows user. This user must have sufficient privileges to access the network resource required for printing the report."

Report Scheduler Service Manager

With **Report Scheduler Service Manager** installed, the user is able to control the **Report Scheduler Service** from the desktop. The user does not have to go to the Services folder in the Control Panel to control the service.



Once the program starts running an icon is displayed in the system tray.

Right click on the icon to choose commands to control the Report Scheduler Service.

You can also control the Service from the main window of the application.

- 1 **Restart Service** - Click on this button to restart the service. If the Service is running it will be stopped and restarted.
- 2 **Refresh Service** - The Service refreshes automatically on a timed interval of 5 seconds. Clicking on this button will refresh the service immediately.
- 3 **Set E-mail** - Click this button to define the e-mail settings which enables automatic e-mailing of reports. On the **E-Mail Settings** window fill in the following fields.
 - a) **SMTP Server URL or Address** - The IP Address or URL of the SMTP Server. This host name can be any valid SMTP server with the capability of supporting standard SMTP mail formats.

- b) **User Login Name** - The login name to the SMTP server.
 - c) **Password** - Enter the password to the SMTP Server.
 - d) **SMTP Port Number** - The industry standard port number for SMTP Server. Usually it is port 25.
 - e) **From E-Mail Address** - The address typed here will be displayed in the 'From' area of the E-mail that is generated.
 - f) **From Name** - The name that will appear on the E-mail that is generated.
 - g) **Reply To Address** - If a reply is made to the E-mail that is generated by the System Processor, this E-mail address will appear automatically within the new E-mail.
 - h) In the empty field enter the text for the e-mail. This appears on the body part of the e-mail automatically.
- 4 **Start/Continue Service** - Click on this button to resume the Service once it is stopped.
 - 5 **Stop Service** - Click this button to stop the service.
 - 6 **Auto-start service when OS starts** - This option determines the services start up type.
 - 7 **Debug** - If the program is in the Debug mode, additional event log messages appears giving you more information about the functioning of the Service.
 - 8 **Apply Changes** - Once you make your selections, click this button to save the changes you made.

Report Scheduler

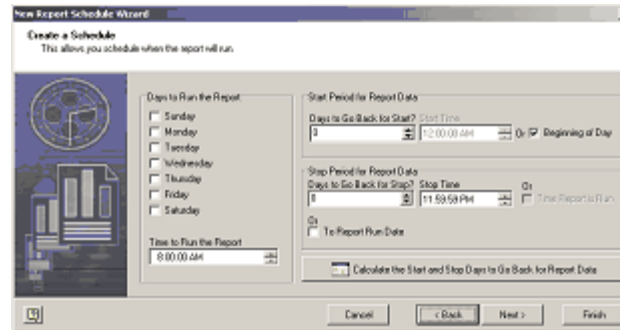
Overview

The Report Scheduler module is where you create, edit and delete schedules. Make your selection using the tool bar icons or by selecting from the File menu. The grid window allows you to view important schedule information at a glance.

Creating a new Schedule

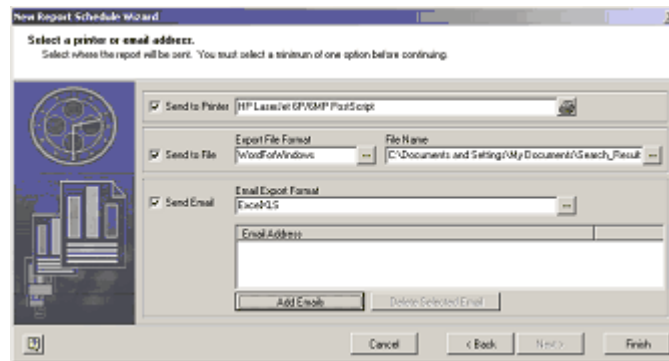
- 1 On the main window, click on the **New Report Schedule** icon to launch the wizard. All reports that have been defined in the Report Launcher module will be shown in the Report Tree. Clicking the plus icon next to the base report heading will display a list of available reports for that category including all derived sub-reports.
- 2 Once a report is highlighted, it appears in the **Selected Report field**. *The Selected Report field can be modified and it is recommended that you give your schedule a meaningful name.* It is important to note that when a derived sub-report (user defined report) is highlighted, its base report name is displayed in this field.

- 3 The next step is creating a schedule for this report. Make appropriate selections.



- a) **Days to Run Report** - Under *Days to Run the Report* place a checkmark next to each day on which you want to run the report automatically. For example, if it is a weekly report that is due on Monday, place a checkmark next to Monday.
 - b) **Time to Run Report** - Default time is preset to 8:00 AM. To change the time, type over the hour, minute and second fields or use the up and down arrows. For this example, we will change the time to 6:00 AM.
 - c) **Start Period for Report Data**
 - **Days to Go Back for Start** - This field is used to calculate how many days that the report should go back to gather information; it is also referred to as the starting date range.
 - **Start Time** - This field defaults to the either 00:00:00 or 12:00:00 AM depending on the time format set in your Regional Settings. To change this time, remove the checkmark from the field titled Beginning of Day.
 - a) **Stop Period for Report Data**
 - **Days to Go Back for Stop** - This field is used to determine the cut off day and time for the end of the report. This is also called the Stopping Date Range.
 - **Stop Time** - This field defaults to 23:59:59 or 11:59PM. Remove the checkmark to specify a specific time of day.
 - a) **Report Run Date** - This field is associated only with the Stop Time and means that the data is current, up to the moment the report is launched.
- 4 Use the **Calculator** button to quickly determine the correct days for the start and stop of the report.
 - 5 Calendars offer a simple way to select the *Report Run Date*, the *Report Start Date* and the *Report Stop Date*. To make a selection, click on the date. It will become highlighted in blue. For this example, we have chosen Monday, January 7th as the Run Date, December 31st as the Start Date and January 6th as the Stop Date. The report will gather and reflect all data from Monday, December 31st through Sunday January 6th. The report will begin to generate on Monday morning at 6:00AM and will be waiting at the printer at the start of the business day.
 - 6 Using this shortcut helps to eliminate confusion. Notice that it has calculated the number of days for you. Under the Start Date calendar, it reads "7 Days Back". Under the Stop Date Calendar, it reads "1 Day Back".
 - 7 Click **OK** to return to the schedule screen. Click **Next** to select a printer or e-mail address to send the report.

- 8 **Selecting a Printer** - Select **Next** to export the report(s) to a file or e-mail address. You can also choose to send the report to a printer.



- 9 If you wish to send the report(s) to a printer, select **Send to Printer** check box. To browse all available printers on your computer, select the printer icon. Highlight the printer from the list and click **OK**.
- 10 Select the option **Send to a File**. Next, choose the file format. Click on the expand button near the field **Export File Format**. The Report Scheduler application supports a wide variety of file formats include but not limited to html, rich text format, Excel, Acrobat pdf, xml, word for Windows, Lotus and so on.
- 11 From the **Select a File Export Format** window, choose the format and click **OK**. The report will be saved in the format that you selected here.
- 12 Select a file name. Click on the expand button to specify the path where the report is going to save.
- 13 Another option available is to send the report(s) via e-mail to the recipients. Enable the option **Send E-Mail**.
- 14 Select the file format using the expand button. The report will be sent to the recipients the format you specified here.
- 15 Now, select the e-mail addresses. You must select at least one e-mail address. When you click **Add E-Mail Addresses** the system displays the e-mail addresses stored in the system using the E-Mail Address Editor program. Click on **Delete E-Mail Addresses** to remove any address from the list.
- 16 Select **Finish**. A weekly report has been defined and will automatically run every Monday morning at 6 AM.

Edit a Schedule

The Edit Report Schedule Wizard opens allowing the user to modify fields of an existing schedule.

Delete a Schedule

The delete icon will eliminate a scheduled report.

Report Launcher Settings

CHAPTER 32

Introduction

A system administrator or other authorized user can create, modify and delete new report groups and organize existing base reports using Report Launcher Settings. These settings let you arrange the system reports to display in the manner that best suits your practice. The constraints you set on reports here help to ensure consistency and minimize the need for operator input while building reports.

Accessing the application

- 1 Open the system launcher software by double clicking on the launcher icon on your desktop or go to **Start>Programs>Schlage SMS>Schlage SMS**.
- 2 Enter your assigned user ID and password.
- 3 In the **System Launcher** window, double click on **Report Settings** icon.

Report Groups and Sub Reports

Overview

The **Report Settings** are divided into two tabs. When you open Report Settings, the system displays the options available under **Reports Editor** tab. If you want to go to the next tab, click on **General Settings**.

The **Report Editor** tab is used to add or modify **Report Groups** and **Base Reports**. New reports (created in Crystal Reports Version 8) are automatically added to the **System Security** module and should be assigned the proper privileges. As new Report Groups are added to the database, they will automatically appear on the Report Editor display window.

The **General Settings** tab determines how many quick launch items appear in the **Report Launcher** module. The default is 10, however, you may enter any number between five (5) and fifteen (15).

General Settings

The General Settings tab determines how many quick launch items will appear in the Report Launcher module. The default is 10. However, you may enter any number between 5 and 15.

Creating a new Report Group

- 1 Click on **New Group** to open the **New Report Group** window.
- 2 Enter a description for the report group. This is a required field. It is recommended that notes also be entered. This feature can be used to create specific sets from all available reports. For this example, we will create a new group called "Daily CIM Reports".
- 3 Now you can select base reports and assign it to the new report group.

Creating a new Sub Report

This feature is used for organizing reports under a common Report Group. This feature makes it easier for the end users to find a report that they frequently use. It also helps to specify daily/ weekly reports that should be generated or to allow users to view and print only certain report.

- 1 Click on **New Base Report** to launch the **New Base Report** wizard.
- 2 In the **New Base Report** wizard, enter a name for the report in the description field. You can enter additional information in the **Notes** field. Click **Next** to continue.
- 3 In the next step, select a report and assign it to a report group. To locate the report file, use the browse button to open the Schlage\Data\Reports folder; select a report by clicking on it to highlight, then choose **Open**.

Note: If you are not sure of the report file name as it is displayed in the Report folder, the naming format can be obtained from the Report Information file under Schlage\Data\Reports directory. It is also located in the footer section all reports printed under the Report *Launcher* module.

- 4 The report file name is saved in the Description field. Use the drop down menu in the **Report Group** field to assign group membership. We have now used an existing report and assigned it to the new report group we created.
- 5 On the next screen, choose options from **General and Device Selections**. Checking one of these options indicates that the report is based on the selected cardholders, areas, devices etc. The device selections include, Readers/Offline Locks, Relays, Contracts, Controllers, CIM Ports, CIMs, and Workstations. You do not have to include selections that will not pertain to the report. In many instances, you do not need to include general or device selections.
- 6 Click **Finish** to complete the process. You can see the new base report created under the report group you previously chose.

Editing and deleting Report Groups

- 1 In the main screen, under the **Report Editor** tab, expand the tree of a Report Group. Highlight your selection and right click or double click on it to Edit or **Delete**. This activates the **Report Edit** screen.

Note: You cannot delete default groups or reports.

- 2 To delete a report group, right-click on it and select **Delete** from the menu. A confirmation message is displayed. Click **Yes** to confirm your action.

Editing a Base Report

- 1 To edit a base report, select the report and right click on it. The **Report Edit** window is displayed.

- 2 Report Edit window has two tabs. The **General** and **Selections** tabs. Modifications are entered in the fields of these tabs. In the General tab you can change the description, notes, report file and report group. The Selection tab lets you change the General and Device Selections. Use the browse buttons to find a different report name or group.

Deleting Reports

Only those report groups and sub reports that have been user defined may be deleted. The Schlage software will not permit deletions of default report groups or base reports.

- 1 To delete a report, highlight the report in the **Report Editor** tree, right click and select the **Delete** option.

Report Launcher

CHAPTER 33

Introduction

The **Report Launcher** module allows operators with the proper security privileges to create, add and generate comprehensive reports. The Schlage software provides report groups for Alarm History, Archive History, Audit Trail, Cardholders, Database, Guest Pass, History, and Transaction History reports. Report wizards make the creation and output format fast and simple. You may print and/or export reports to other applications, store to disk or send to mail recipients, as well.

The **Report Launcher** is used to generate reports that contain specific criteria. All available reports reside under a group name in the Report Tree. There are seven Report Groups; they are Alarm History, Archive History, Audit Trail, Cardholder, Database, Guest Pass and Transaction History reports. Additional Report Groups and reports can be created in the Report Settings module.

The main window contains the Menu bar, Shortcut icons, Quick Launch drop down option and the Report Tree.

Accessing the application

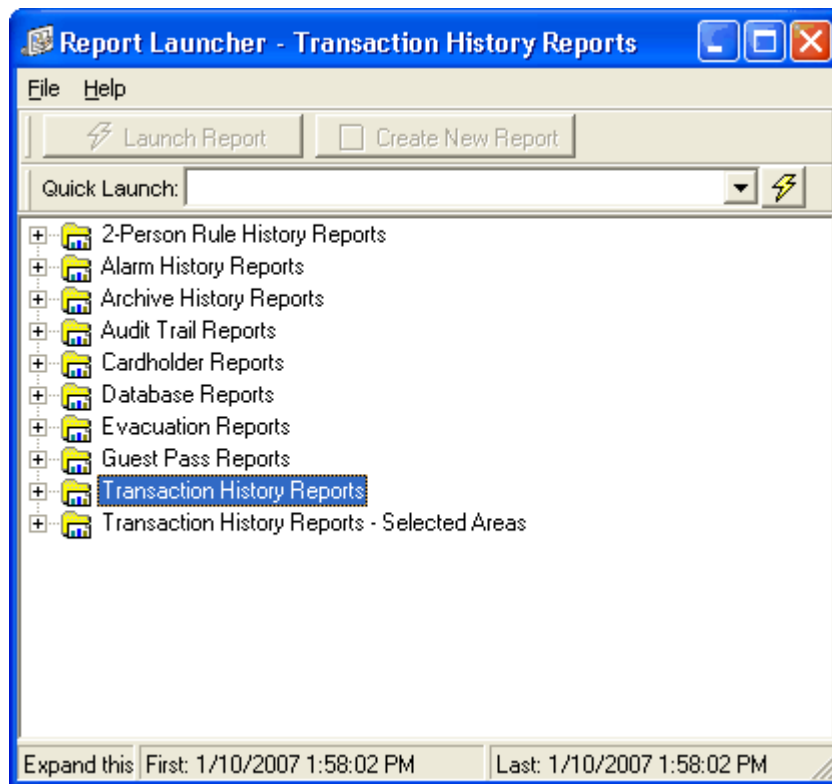
- 1 Open the launcher by double clicking the Launcher icon on your desktop **Start>Programs>Schlage>Schlage SMS**.
- 2 The login window, opens. Enter your user ID and password.
- 3 In the System Launcher window, double click on **Report Launcher** icon.

Working with Report Launcher

Overview

Report tree view

The Report Tree displays Report Groups with its associated Base, Derived and Derived Sub-reports that can be generated. Base reports are pre-defined Schlage reports. Derived reports are used to create sub-reports; they are represented by a yellow, lightning bolt with a red circle. Derived Sub-reports and Base reports can be launched immediately and will have an icon.



Report Groups

Under every Report Group in the tree are base and derived reports and any pre-defined (user created) sub-reports. New report groups can be added using the Report Settings application.

Base Reports

These reports are pre-defined in the **Schlage SMS** software and therefore need no further user input except a Date and Time selection. Base Reports can be immediately launched and are indicated by a yellow lightning bolt. An example of this type of report is the Cardholder Information Report – All Cardholders. Since all cardholders are reported, it is not necessary for the user to select any cardholders.

Derived Reports

Derived Reports are identified by a lightning bolt with a red circle. They cannot be launched. Instead they use Base report criteria and require selections to be entered that define a user created sub report. Some examples of selections are cardholders, areas, readers, relays and contacts.

Derived Sub Report (User created)

The plus sign next to a Derived icon in the Report Tree indicates that a user created sub-report has been defined and is available. Expand the tree and the report will have an icon. This type of report is created by highlighting a Derived Report, choosing Create New Report and supplying information in the New Sub Report Wizard. Once defined, it can be launched and will use the selections made in the wizard for the result set. No other operator will be able to launch, delete, or edit these reports except for the operator who created it. The yellow, lightning bolt icon means that the report can be launched immediately

Launching a Report

In order to launch a report, there must be a yellow, lightning bolt graphic next to the description. This is the indication that the report can be generated.

- 1 Highlight the description within the Tree and click the **Launch Report** button or right click and send the command from the sub menu or select **File>Launch Report**.
- 2 If a **Date** and **Time** is required, an entry dialog will appear. Once this information is entered, the report will be displayed in its own window.

Quick Launch feature

The Quick Launch feature makes it easy to run recently launched reports. By default, it keeps track of the last ten reports that have been launched (not using the quick launch).

You can then easily use the drop down list in the combo box to select one of these reports and launch it by clicking the yellow, lightning bolt button to the right of it. You will also find a list of these reports under **File>Recently Launched Reports**.

Printing a Exporting Reports

Printing a Report

- 1 To print a report, just click on the printer icon shown in the toolbar of the report output display screen. The default Windows printer selected will be used here. The print range, collate option and number of copies may be selected.

Exporting a Report

Also located on the toolbar is the Export button, which will open the Export window. This feature allows you to choose a format and destination for exported reports. The format and destination choices for these files are specific to the applications you have installed as well as the version of Crystal Reports.

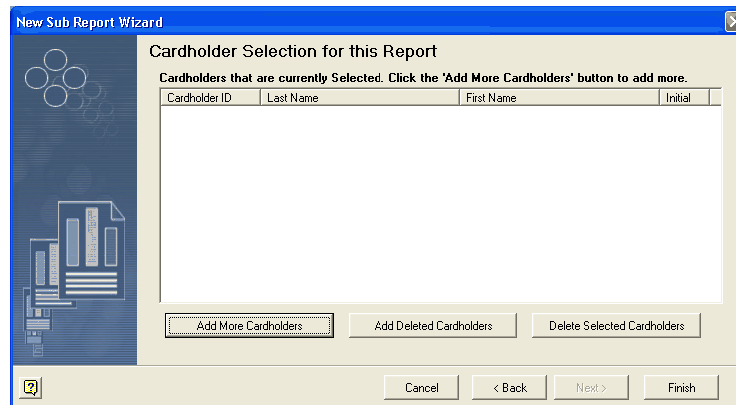
Adobe Acrobat, Word for Windows and Excel files are among several file types supported by this Crystal Report utility.

Note: Schlage SMS version 5.1.4 do not support formats like Character separated values, Crystal 7.0, Data Interchange Format DIF, Various Versions of Excel, Lotus selections, ODBC and Paginated Text.

Creating a new Sub Report

- 1 Creating a new report is easy. Simply click on the appropriate Derived Report (indicated by a lightning bolt with red circle). For example, if you want to run a cardholder information report on only a few cardholders, select the Cardholder Information Report - Selected Cardholders.
- 2 Once you have highlighted the appropriate report, click **Create New Report** or right-click on the highlighted report, and select **Create New Sub Report**. You can also start the wizard by double-clicking the derived report. When you click the button, the New Report Wizard will display. Step through this wizard until all of the appropriate selections have been made. The wizard will not let you finish until all of the required data has been entered or selected.
- 3 The first step of the wizard is to enter the **Description** and **Notes** of the report. The description is displayed in the tree and helps you remember what the report is. You have 64 characters of space for this field, which is enough for a good description. Remember, the base report also has a description, which further defines what this new report is. If you need a very elaborate description, you can use the **Notes** field, which allows 255 characters.
- 4 Launch this Report after it is created option allows you to immediately begin to run the report using all of the criteria you have selected in creating it.
- 5 The remaining steps of the wizard will ask you to select one or all of the following: Cardholders, Areas, Categories, Readers, Relays, Contacts, Controllers, CIM Ports, CIMS, and Workstations. Credential function is displayed for only CM Locks.

For example, for a selected cardholder report, you would see the following window:



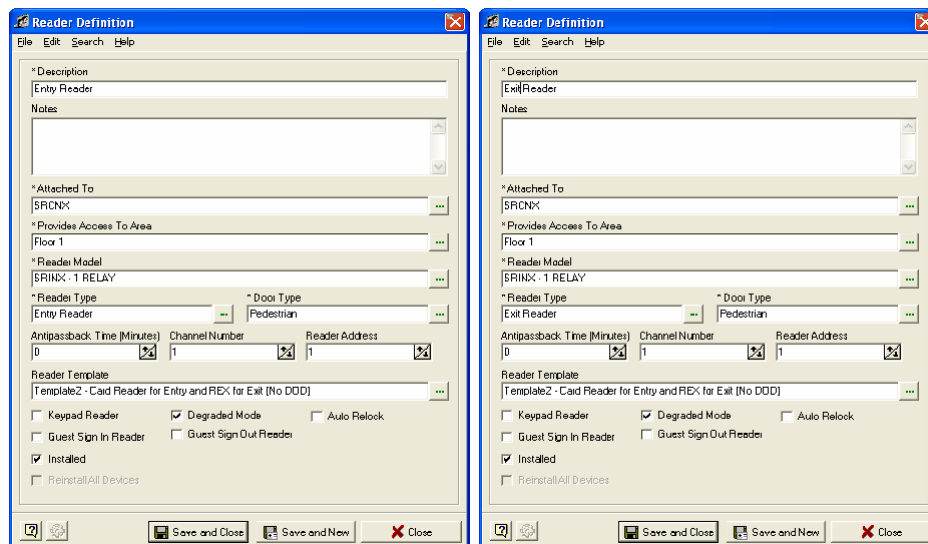
- 6 In this step, the system is asking the user to add cardholders to the report. These cardholders will be used as the data for the report.
- 7 When you click **Add More Cardholders**, the Cardholder Search wizard will display. The Cardholder Search wizard allows you to search for cardholders within the database and select them. You must type in all or part of the last or first name and then hit the enter key. The cardholders that match the search criteria will be displayed on the bottom. Use the Find Now button to see the entire list of cardholder.
- 8 Highlight cardholders (holding the Ctrl key as you click) and hit the enter key or choose **OK**.
- 9 These cardholders will be selected for the report and will show up in the initial selection wizard screen. All of the cardholders that are displayed in this screen will appear in the report.
- 10 Click **Finish** to launch the report. If the **Launch Immediately** button was checked in the first step, the report will be launched automatically.

Note: The method of selecting Devices and Areas is a little different, but easy to use and follow. You will see these steps only if the report requires those selections.

Creating Evacuation Reports

Evacuation reports allow the users to make sure that the cardholders are evacuated safely after an emergency. The purpose of the evacuation report is to list all cardholders who have not yet presented their badge at an “exit reader” after an emergency. This list is intended to aid emergency workers in locating all employees after any type of disaster.

Entry and Exit readers - Since the emergency procedures may be run on a single building, it is necessary to identify the readers within the endangered building. To facilitate the identification of readers, all evacuation reports will require an “entry” reader and “exit” reader.



While defining readers, select the reader type as “Entry Reader” and “Exit Reader”.

These readers will be used to register cardholders (employees). It's also anticipated that within the evacuation procedures there will be instructions for employees to swipe their credentials at an exit reader.

Now while creating the report, in the **New Sub Report Wizard>Reader Offline Lock Selection for this Report** section, add the entry and exit readers.

Generally speaking, the Evacuation Report lists all cardholders who have used their credential at the entry readers and have not yet presented their credential at the exit reader. The report will list the cardholders name and the date/time, area, and reader of the last access attempt (valid or invalid). The report will be ordered by the cardholder name: Last name, first name, and initial.

Editing a Sub Report

- 1 In order to modify a sub-report, highlight the report name, use the right mouse button and select **Edit Report** from the menu options.
- 2 The **Report Edit** window is displayed. The Description and Notes fields can be modified. The Report File Name cannot be changed, however, it is displayed for reference. You will also find the Date Created and Date Last Run fields here.

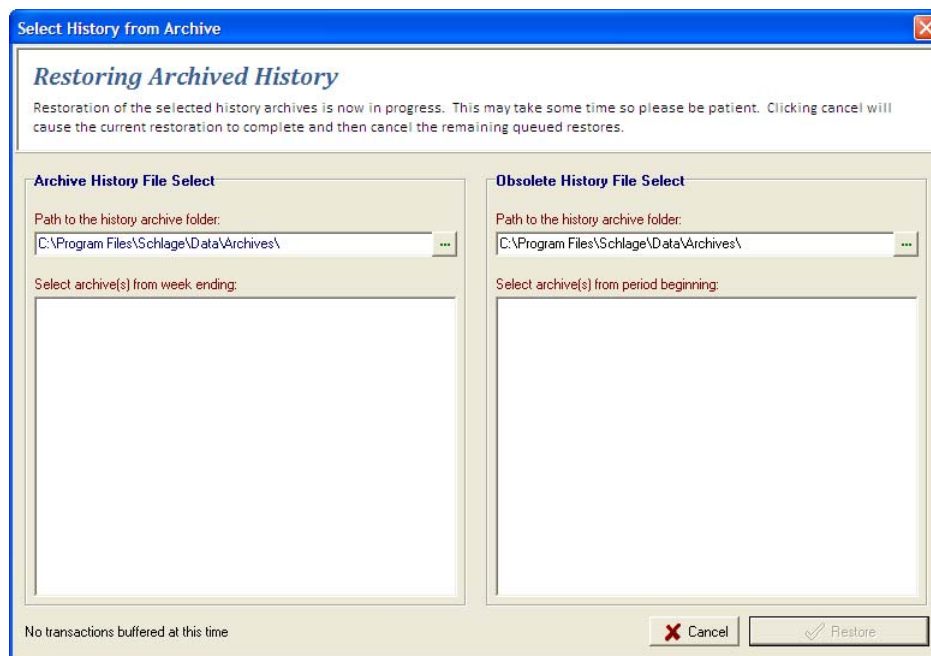
Deleting a Sub Report

- 1 Highlight then right-click the report you want to delete and click the **Delete Report** menu option or right click and select Delete Report from the menu. The software will not permit the deletion of Base and Derived reports.

Restoring Archived History

Restoring Archived History

This new feature allows you to restore current and legacy history files. To access the feature open the Report Launcher and go to **File>Restore Archived History**.



- **Path to the history archive folder** - use this field (in either the Archive History or Obsolete History sections) to specify the location of the archive folder.
- **Cancel** - Closes the window without restoring history.
- **Restore** - Restores the selected history file.

Audit Trail-Settings

CHAPTER 34

Introduction

The **Audit Trail Report** program allows the user to conveniently monitor any modifications made to your database. Using the **Audit Trail Control Module** the system administrator can preset the options that you wish to monitor and control the flow of information in your **Audit Trail Report**. Virtually all Area Access, Area, Cardholder, Badge and Timezone activities can be organized and viewed with the two modules that comprise the Audit Trail Reporting. You could widen or limit the scope of the report so that it is possible to view all the records that fulfill certain characteristics. It is important to remember that both the modules in Audit Trail are intrinsically related.

Note: This is a control module. It is recommended that permissions be granted to administrators only.

Accessing the application

- 1 Open the **System Launcher** by double clicking on the launcher icon on your desktop or select **Start>Programs>Schlage SMS>Schlage SMS**.
- 2 Enter your assigned user id and password.
- 3 In the System Launcher window, double click on **Audit Trail Control** icon.

Overview

The **Audit Trail Control** module allows the user to set the type and extent of information that the Audit Trail Report will collect. Before you run a report, you need to select the fields in the Audit Trail Control that will be considered requisite data for reporting.

When you open the Audit Trail Control, you can see that the main window is divided into sections: Duration of History (in Days), Select Data Table, Record on Insert and Record on Update.

Note: Audit Trail reports can also be generated using Report Launcher program.

When **File>Audit Trail Enabled** option checked, reporting is turned on. If unchecked, no audit trail will be created.

Settings

Duration of History (in days)

The Duration of History (in Days) is an important field and makes a great impact on the amount of data recorded. You have a choice between 0-365 days while the default is 14. This sets the length of the time period that the computer keeps the records of all inserts and updates of data. After the amount of days specified, the auditing reports of the records will be deleted. If you set a 16 day duration that means you will not be able to create a report that includes any data beyond the 16 days range in the **Audit Trail Report**.

The length of the duration is completely a matter of choice. The longer the duration, the more data compiled and the larger the report. However, in most instances, you will not need to keep your records for more than a few weeks because the importance of this information to security might be irrelevant by this time. Of course, you may want to generate weekly or monthly paper reports that are kept in a binder.

Select a Data Table

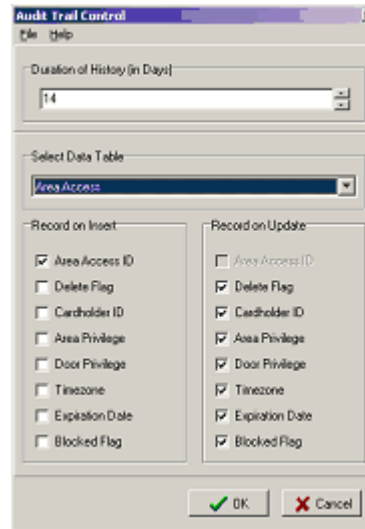
Here select the data table from the drop-down bar, which allows you to set the input and update options for the various data tables. There are six data tables available:

- 1 Area Access
- 2 Area
- 3 Cardholder
- 4 Badge
- 5 Badge Activation/Retirement
- 6 Timezone

These six choices are also the tabs you will see when you run a report in the Audit Trail Report module.

Note: The data table you select in the drop-down determines the type of checkbox options that will be displayed in both the Record on Insert and Record on Update columns below it.

Record on Insert/Record on Update



The above screen capture shows all Area Access fields that are available to display on the report when a record is originally created (Insert) and when modifications are made to that record (Update). Each data table has a specific set of options that determine how much and what kind of data will be recorded from the records in the database.

The record on insert checkbox options define how much information will be recorded whenever you create a new record in the database. Record on update collects data whenever you change any part of a pre-existing record in your Schlage Access Control database.

You will see similar options among the different Data Table checkbox options and within each Data Table the Record on insert options exactly mirror the Record on Update. So you may select an option, such as to record the Cardholder ID on insert, while not choosing the same option for Record on Update. These individual variables are determined at your discretion. The checkbox options are simply those fields you normally define when creating a record. For example, whenever you create a badge for a cardholder, you must define such fields as Stamped ID, Encoded ID, Issue Code and Badge Layout.

If you wish to record any inserts or updates on these fields, you must specify in the Badge Data Table by selecting the corresponding checkboxes.

Audit Trail Report

CHAPTER 35

Introduction

Audit Trail Report is a program that allows you to conveniently monitor any additions, deletions and changes made to your database. This module is used to create reports and view differences in the data tables. Virtually all Area Access, Area, Cardholder, Badge and Time zone information can be organized and viewed. For example, if an operator mistakenly deleted an Area that in turn affected cardholders and their Area Access, you can quickly determine which user was responsible, the date of the change, the Area name, the original value and the updated value.

Accessing the application

- 1 Open the **Schlage SMS** by double clicking the Schlage SMS icon on your desktop or select Start>Programs>Schlage SMS>Schlage SMS.
- 2 The login window, opens. Enter your user id and password.
- 3 In the **System Launcher** window, double click on **Audit Trail Report** icon.

Generating an Audit Trail Report

Overview

The **Audit Trail Report** window displays three categories with sub-fields that need defining. They are **Report Dates Available**, **Begin Report** and **End Report**. These fields set the parameters of your Audit Trail Report.

Audit ID	Date Of Change	Operator
28	11/22/2006 5:13:53 PM	USR
29	11/22/2006 5:13:53 PM	USR

In the **Audit Trail Control** module, the “**Duration of History**” option determines the amount of data that is stored in the system. After the amount of days specified, the records are deleted from the Audit Trail tables. If the duration is set to 14, that indicates you will not be able to create a report that includes data beyond the 14 day range regardless of what is entered in the **Beginning Date** and **Ending Date** fields of the Audit Trail Report module.

End Report

The **End Report** option allows you to delineate the utmost time limits that your report will collect information. In other words, it determines the last day to be included in your report. Both the Ending Date and Ending Time field define it.

The **Ending Date** field defaults to the current date, but this can be changed to an earlier date if you want to define a specific time period (for example, a Beginning Date of January 1st to an Ending Date of January 15th. The Ending Time field defaults to 11:59:59 pm but this can also be changed to your specifications.

Run Report

After all the categories are defined, click the **Run Report** button on the upper right side of the window and it will gather information from the system and organize the report along your specifications.

Refresh Report

When you change any of the criteria of the fields, click the **Refresh** button to generate new data.

Understanding a Report

After a report has been run, the information captured from your Schlage database will be displayed in column and grid format on the bottom of the screen. This information in the grid display can be viewed six different ways, each represented by a tab. These tabs are: **Area Access**, **Area**, **Cardholder**, **Badge**, **Badge Activation/Retirement**, and **Timezone**.

The fields are displayed in grid format under the selected tab. One record created in the Cardholder Definition module can easily result in ten to fifteen rows displayed on the Audit Trail Report.

Note: Each individual record you create, such as a cardholder, has many fields that can be monitored by the Audit Trail Report. Whereas you may have created only one Cardholder, the Audit Trail Report can display all fields associated with that record, such as First Name, Last Name, Cardholder ID, etc. as shown in the following examples.

Each tab in the Audit Trail Report represents a Table. Many of the columns titles, which mirror fields of your records, are found in more than one tab. Click on each tab to see the corresponding database changes that are made. The report shows data of change, the operator's user id, activity (insert or update), and cardholder's name.

Column Name Definition

- 1 **Area** - This lists the Area description as defined in the software.
- 2 **Audit ID** - This is the number assigned by the system to the specific record field (entire row) in the context of the whole Audit Trail Report.
- 3 **Cardholder** - This displays last and first name of the cardholder.
- 4 **Column Name** - The actual title of the field that was created, changed or deleted such as Cardholder ID.
- 5 **Data Table** - This defines the table name where activity was recorded in the Schlage software. If a badge was activated or retired, the table name will display in the Data Table column of the Badge Activation/Retirement tab.
- 6 **Date of Change** - This reflects Date and Time of inserts or updates that were made.
- 7 **Encoded ID** - This is the unique number assigned to a cardholder's badge. This number is physically programmed into the badge and is read by the reader and used to identify the cardholder and their access privileges.
- 8 **Operator** - This shows the User Login name that made the change.
- 9 **Operation** - This column lists the type of activity that occurred in the database. *Insert* will be listed when any new records have been added; *Update* is listed when you have altered an existing record and *Delete* indicates that an operator has removed record.
- 10 **Original Value** - This will list initial properties of the record you are viewing. For newly created records (Insert), the Original Value will be blank.
- 11 **Updated Value**: This shows whatever modifications have been made to pre-existing records. You can use this to compare the new Updated Value with the previous value given to the record, which is shown in the **Original Value** column.
- 12 **Referencing Timezone** - This is the name of the Timezone that was deleted.

Rearranging and sorting column titles

Column titles can be placed in any order that is convenient to the user. Simply drag the column title and drop it to a new location. To sort in ascending or descending order, click in the title bar.

The sort order is viewed on the bottom, left of the screen. Total Rows is written to the left of the sort order.

Setting dates

In order to generate an audit trail report you need to specify the following fields in the Audit Trail Report program.

- 1 **Report Dates Available** - The first category is called Report Dates Available. This has two fields, Date of First Entry (UTC) and Date of Last Entry (UTC). These fields represent the absolute limits of your date definitions; obviously you cannot ask for reports of changes in your database before it was installed or beyond today's date. Therefore, you are limited to the period of time between these two dates as listed in the fields.
- 2 **Begin Report** - Begin Report has two fields. You can set the extent of your report by defining in the **Beginning Date** field the exact day from which you want to check all system activity, though the default is today's date. You further clarify this with the next field, **Beginning Time**, which defaults to 12:00:00 a.m. It is important to remember that the number of days you set in the **Duration of History** (in Days) in the Audit Trail Control module will dictate the absolute limits of when you can gather records. If you set the duration for 14 days, a Beginning Date before 14 days from today is invalid because all auditing records beyond 14 days have been deleted.

CIM

CHAPTER 36

Introduction

The **Communication Interface Module** or **CIM** is a program designed to issue all database changes and gather information from the reader controller. The CIM gathers information and stores it in the proper history files. The CIM phone lines, direct cabling or TCP/IP communication protocols may all be used with the SRCNX Boards.

Note: When setting up the CIM, it is imperative that you do not deviate from the instructions given. This module will not function properly if the instructions given are not followed.

Settings

Creating a CIM Log Directory

The administrator needs to create a CIM log directory where all CIM log files will be stored.

Note: The CIMLOG directory is not necessary, but it is recommended so that the text files are organized in one location. This will make it easier to locate the files for troubleshooting purposes. Also, when creating the directory keep in mind that the directory name is not case sensitive.

- 1 To create the directory, proceed to your Windows desktop. Double click on the My Computer icon, and then double click on the C:\ drive.
- 2 Click on **File>New>Folder**. On the newly created folder type in "**CIMLOG**".

Starting the CIM

The CIM starts automatically when the workstation is turned on.

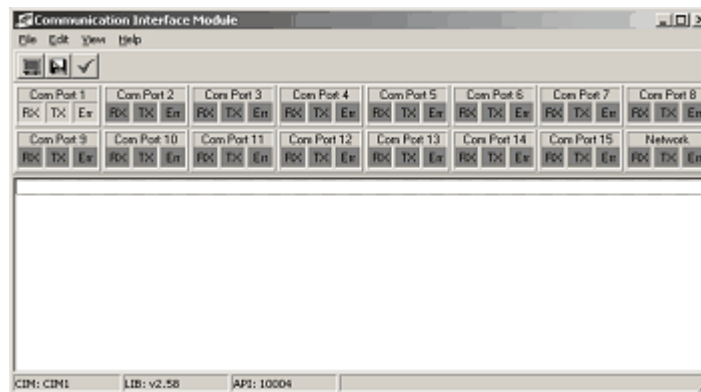
Follow these steps to start the CIM automatically.

- 1 Open the **System Launcher** by double clicking on the **Schlage SMS** icon on your desk top.
- 2 In the **Log In** window, enter your assigned user id and the password.
- 3 The **System Launcher** window is displayed.
- 4 Open the **System Security** application.
- 5 Click on the **Startup** tab. Select **Edit>Add**. All the modules that can be added to the Start up option are displayed. Select CIM and click **O.K.**

- 6 After clicking on the **CIM** icon in the **System Launcher**, a splash screen is displayed indicating the Access Control System is initiated. Once this process is complete, the **CIM** main screen will open and you will be ready to set up the **CIM**.

Note: This module should run only on the workstations that are assigned as CIMs.

Main screen view



The CIM setup is done from the main screen. After setup, the main screen is used to monitor the CIM. Prior to setup, all the Com Port display is dark gray. Once you have attached the SRCNX board to and setup the Com Ports, the color of the ports that are active will reflect the current status. This feature enables you to identify which Com Ports are active at a glance.

Note: By grabbing the side of the CIM Window, you can change the size of the com port Display or the size of the message display, allowing not only to change the shape, but also to view as few or as many Com Ports as desired (up to 16).

Options

- 1 **Select Log File** - From the File menu select the option **Select Log File**. This opens the **Log File Select** window to choose a location and name for the CIM log text file
- 2 **Log Status** - From the **File** menu select the option **Log Status**. This is to enable\disable logging to the above text file

View Settings

In the **View** menu you can adjust the viewing window of the CIM to meet your specific needs. By clicking on an item and placing a check mark next to it, you will activate that item. To deactivate, click again and remove the check mark.

- 1 **RC Status** - To display all of the Com Ports, which allows you to open the **Com Port Expansion** window, select **View>RC Status**. The default is on.
- 2 **Status Bar** - To view the status bar at the bottom of the CIM window, select **View>Status Bar**. The default is on.

- 3 **Toolbar** - To view the tool bar in the CIM window click **View>Toolbar**. Removing the check mark will make the toolbar invisible.
- 4 **Status Messages** – This option opens the **Set Message Logging Priorities** window to the default communications tab. Settings made from this menu apply to all defined Com Ports in your system. General and Networking tabs also contain the choices for turning messaging on or off, logging it, pausing it, and what level of messaging will be displayed.

Note: You cannot set **Communications** messaging to Show All system-wide. Individual Com Port communications can be set from the **Com Port Expansion** window.

- 5 **Report Update Complete Transactions** - Enable this option in the View menu to report an update to an RC board is complete. This is useful for troubleshooting and monitoring status on multiple boards.
- 6 **Copy Monitor Tables** - This option opens the **Copy Monitor Settings** window to the default Customer Supplied DLL tab. Details of this feature follow later in this chapter.
- 7 **Clear Status Display** - To clear the display grid of all the information select **View>Clear Status Display**.
- 8 **Automatic Updates** - To update the controller boards automatically when the CIM information is changed, select **View>Automatic Updates**.

Note: This feature could be turned off when major changes are being made, such as adding a new Area and transferring all devices and cardholders into it. In this case, Automatic Updates would be disabled until all changes have been entered and the update is completed at an off-peak period of the day or evening; then re-enabled.

- 9 **Display Status** - To allow all messages to be displayed in the CIM window, select **View>Display Status**. The last message will always be highlighted at the bottom of the screen. When you remove the check mark, no new messages will be displayed and the scrolling will stop. You will only view the messages that were on the screen before you disabled it and the last message will no longer be highlighted at the bottom of the screen.

Tool bar icons

Status Display Icon - The blue computer icon displays a red line through it, which indicates that status message displays are paused. Click on it to allow the messages to scroll in the window for viewing. This icon has the same effect as the Display Status function from the View Menu.

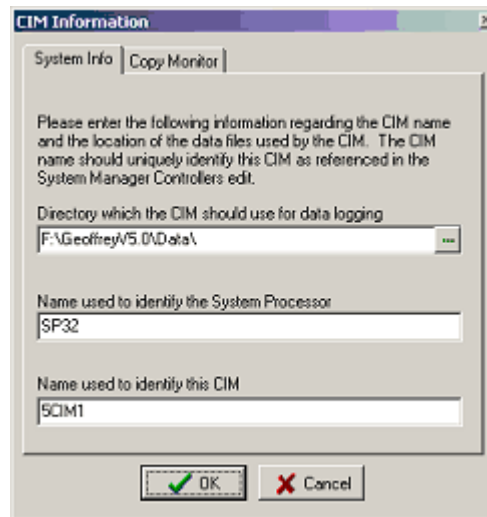
Log Status Icon – this function works the same as the **File> Log Status** feature.

Check Mark Icon – click to place a time stamp and broken line immediately after the currently highlighted message in the status display grid. This will only work while messaging is turned on and may be helpful in troubleshooting.

Note: A hint appears when you place your pointer over a button letting you know what function will take place when you click it.

System Information

The System Information tab contains the location of the database files for the RC Definitions, the Com Port selections, and Data Logging files for the CIM. The information displayed reflects the settings chosen during installation.



- 1 You may change the directory path for the location of the database. The CIM uses this directory for data logging. The default directory for data logging is C:\Schlage\Data\. To select a different directory, click the expand button to open the Select Working Directory window.
- 2 The next two fields are the names used to identify the **SP** (System Processor) and the **CIM**. These can be verified by going to **Start> Programs>Schlage SMS>Registry Entry>System Processes** Tab. These are the names created during the installation.

Note: The CIM name cannot exceed 32 characters.

Status Messages

Message Logging Priorities

- 1 To define the message logging priorities, on the menu bar, select **View> Status Messages**.
- 2 The **Set Message Logging Priorities** dialog box opens to the default communications tab. There are three tabs in the dialog box, each containing the same options. You will have to choose an option for each of the tabs.

Note: It is recommended to click on “Show Medium and high priority messages” on all three tabs when initially setting up Status Messages. Show all Messages is not an available option in the Communications tab. In the **Com Port Expansion** window, choose **File>Message Level>Show All Messages**, which applies to Communications for that specific com port and will produce a CIMLOG useful for troubleshooting.

Set Message Logging Priorities

- 1 **General** - internal messages for the CIM only (Failures and Initialization). Messages appear in **green** in the CIM Message Window.
- 2 **Networking** - Messages sent from other programs to the CIM (Downloader and Override modules). Messages will appear in **blue** in the CIM Message Window.
- 3 **Communications** - Information sent from the CIM to the RC Panels. Messages will appear in **red** in the CIM Message Window.

You may also choose an option on the lower left of the dialog box. The **Log to Disk** option, allows you to save messages to your hard drive for troubleshooting at a later time. **Pause** will stop the message display on the main screen. These options are the same as the logging and display toolbar buttons and **View** menu options.

CIM Start up screen

- 1 Click on a Com Port name to open the **Com Port Expansion** Window. Make sure that the mouse pointer makes contact with the bar above the status boxes RX, TX and ERR. The areas that are not grayed out are the active Com Ports. You can start with any Com Port you wish.

Shutdown/start -up main screen

When all **CIM** Information has been entered, and you have set your message logging priorities, you need to shutdown and restart the **CIM**. This allows the **CIM** to gather all the necessary information from the Access Control System.

The screen looks different than it did during the initial setup. The active Com Ports are now gray not dark gray. This shows which Com Ports are currently active, and the **CIM** is logging files pertaining to each port. You will also see messaging scrolling in the **CIM Message** Window screen. This allows you to view activities for each active port.

Note: Take notice that the active Com Ports will flash. Lime Green flashing indicates everything is fine, yellow flashing indicates that the master board is fine but one or more of the slave boards have problems, and red idle indicates that a direct or master board is not functioning.

Color codes for Com Port Status

- 1 **Solid Dark Gray** - Communications Port not defined.
- 2 **Solid Light Gray** - Communication Port defined (remains light gray during initialization process or if RC Boards are defined incorrectly).

Note: The color codes 3,4,5 apply only to dial up connections.

- 3 **Solid White** - Initialization to dial up modem was successful.
- 4 **Solid Dark Green** - Dial-Up communication to RC Network has been initiated (RC is being called).

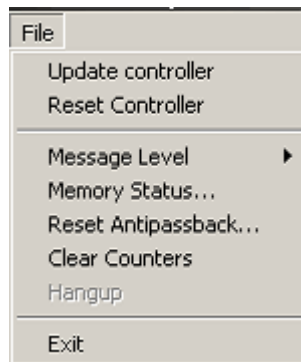
- 5 **Solid Blue** - Modem is waiting for RC to call back.
- 6 **Flashing Light Green** - Communication with RC Network is Proper.
- 7 **Flashing Yellow** - Communication to the Master Board that is connected is proper, but one or more of the downstream slaves are not communicating.
- 8 **Solid Red** - Communications to RC Network has failed.

Com Port Expansion

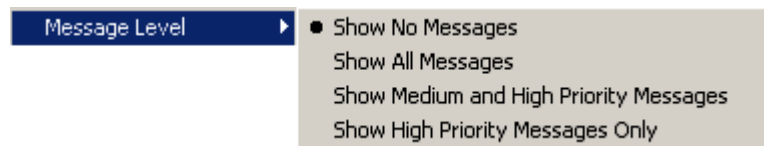
Once the **CIM** has been restarted, you can go onto the next step, the **Com Port Expansion** Window. From the main screen of the **CIM**, click on one of the active Com Ports.

The following screen capture is an example for a **Com Port Expansion** window (The device attached is a Master Controller). A description of all boards connected to a **Com Port** will be listed here under the toolbar. The descriptions of all RC Boards and slaves connected to this **Com Port** are loaded automatically from the Controller Database. The information is displayed is for the highlighted board.

COM Port Expansion File Menu



- 1 **Update Controller** – This will refresh the RC board with any changes since the last update.
- 2 **Reset Controller** – This will force RC to completely reset the memory. All memory will be deleted. RC board will be re loaded.
- 3 **Message Level** – Refers to the Communications messaging for this Com Port only.



- 4 **Memory Status** – Memory status window mainly shows the total memory of the RC board, used memory and how much memory space is available.

- 5 **Reset Anti pass back** – Resets all anti pass back status to neutral.

Controller Memory		Available Storage	
Total Memory	1048576	Transactions:	27795
Used Memory	98808 → 6%	Alarms:	27795
Free Memory	978641 → 93%	Badges with 1 Area:	11591
		Badges with 2 Areas:	10194
		Badges with 3 Areas:	7645
		Badges with 4 Areas:	6116
		Badges with 8 Areas:	3398
		Badges with 12 Areas:	2352
		Badges with 16 Areas:	1798

Object Counts:

Transactions:	0
Alarms:	0
Badges:	0
Area Access:	0

Buttons: Refresh, OK

- 6 **Clear Counters** - refers to the number of transactions and alarms being displayed; it will clear the count and restart from zero.
- 7 **Hang-up** - disconnects dial-up SRCNX connection.

Definition of fields in the COM Port Expansion window

Device Number:	78
Description:	M11101-01-1.3 Downtown Complex MASTER
CIM Name:	SCIN1
Master Controller:	n/a
Channel:	n/a
Address:	n/a
Phone Number:	84968329
IP Address:	n/a
IP Port:	n/a
Callback Numbers:	
Site Codes:	4095
Holidays:	9/2/2003
Timezone:	(GMT-05:00) Eastern Time (US & Canada)
Local Time:	1/14/2003 15:14:17
Connection Status:	Communicating
Transactions:	467
Alarms:	1
Download Status:	Idle
Firmware Version:	5.66
Automatic Updates:	Enabled

- 1 **Device Number** - Determined by the CIM when setup
- 2 **Description** - Name of RC from board definition
- 3 **CIM Name** - Name of CIM from definition
- 4 **Master Controller** - Name of MC board connected to currently highlighted slave board.
- 5 **Channel** - Channel number to which the Master RC is attached
- 6 **Address** - Address of RC
- 7 **Phone Number** - Dial-Up phone number
- 8 **IP Address** - Unique numerical network address assigned to the CIM
- 9 **IP Port** - Port number of IP
- 10 **Callback Numbers** – down arrow will display all callback numbers listed
- 11 **Site Codes** - down arrow will display all site codes listed
- 12 **Holidays** - down arrow will display all holidays defined listed

- 13 **Time Zone** - Regional Time Zone for RC
- 14 **Local Time** - Tells local date and time for RC
- 15 **Connection Status** - Shows if the RC is communicating with the CIM or not.
- 16 **Transactions** - Number of transactions received from RC since CIM has started.
- 17 **Alarms** - Number of alarms received from RC since CIM has started.
- 18 **Download Status - Idle** - CIM is not currently performing any update to the RC
- 19 **Script text** – scripts are shown when the RC is being reset or updated
- 20 **Firmware** – will show firmware version of the highlighted board
- 21 **Automatic Updates** – drop down arrow allows enable or disable the feature, default is enabled.

Note: Automatic Updates in this window refer only to the individual RC board, and should not be confused with the **Auto updates** option under the **View** menu in the main window. When enabled, this board will automatically receive updates of changes the CIM has, when disabled, the board will be skipped from the overall updates and have to be manually updated by the end user through the CIM or the Download Controller module.

Exiting CIM

- 1 From the **File** menu select the option **Exit**. A confirmation message is displayed. Click **Yes** to exit.

System Processor

CHAPTER 37

Introduction

The System Processor module is made up of two separate programs. One is the System Processor Service and the other is the View SP Status application. The service runs automatically when the machine is started and does not require a Windows log in to function. View SP Status is accessed from the Launcher. The System Processor Service is the software interface between the CIM (Communication Interface Module) and your workstations. Its function could be described as communications traffic control. View SP Status is how you interface with the System Processor.

Note: The System Processor is referred as SP throughout this document.

This application is in charge of directing alarms and transactions to their proper destinations. It reroutes, acknowledges, secures and tracks alarms and logs them to history files. The SP can also send alarms as e-mail messages to legitimate e-mail accounts as defined in the Alarm Definition program.

Starting SP

The SP service starts automatically when the computer hosting it is turned on and only stops when that computer is shut down.

To stop the SP service without turning off the computer:

- 1 Go to **Start>Settings>Control Panel>Services** The Services window will open.
- 2 Right click on IR_SP32 and select **Stop**.
- 3 The SP service is no longer running.

To manually start the SP service:

- 1 Go to **Start>Settings>Control Panel>Services** The Services window will open.
- 2 Right click on IR_SP32 and select **Start**.
- 3 The SP service is now running.

Accessing View SP Status

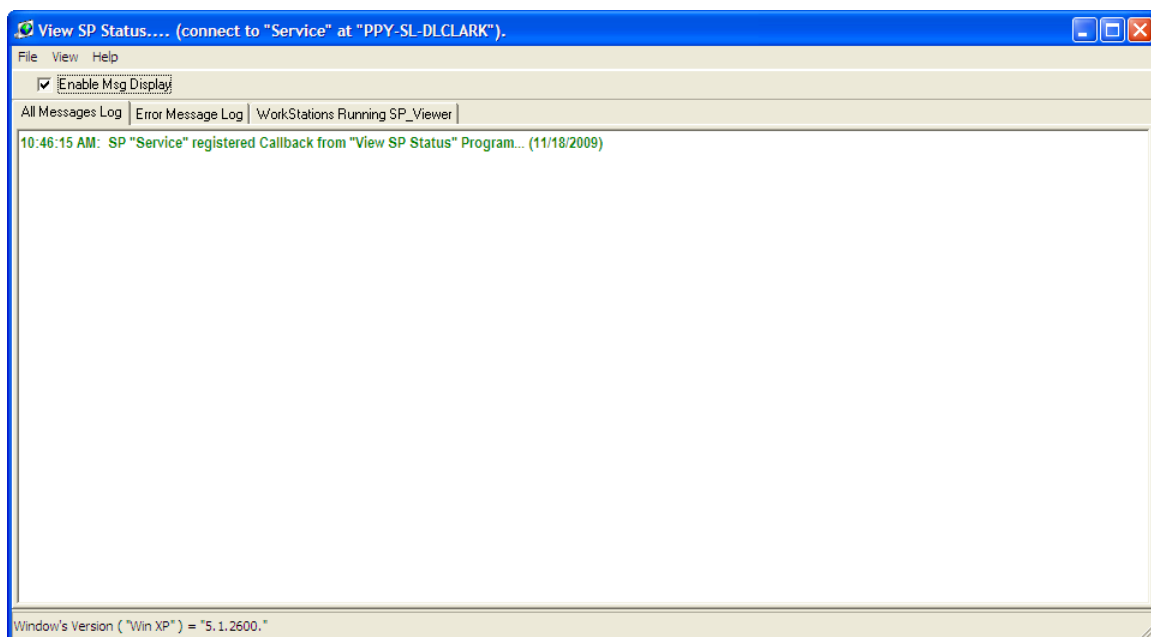
- 1 Open the **System Launcher (on page 42)** software by double clicking on the **Schlage SMS** icon on your desktop.

- 2 Enter your assigned user id and password. In the Launcher window, double click on the **View SP Status** icon.

Note: Any workstation can run View SP Status.

Min screen

All Messages Log



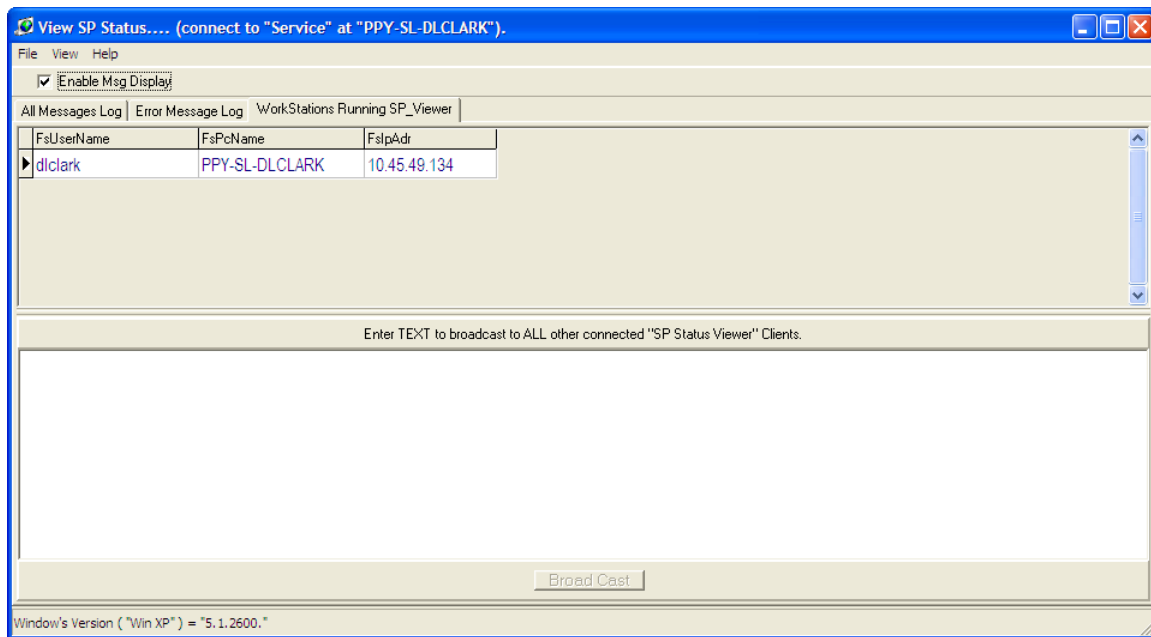
Shown above is the ALL Messages Log screen of the **View SP Status** application before status messaging has been activated. The display grid or the viewing window shows that the **SP** is running and communication with the server is open.

- **General** - Internal Messages for the SP only (failures and initialization). Messages appear in green.
- **Networking** - Messages sent from other applications to the **CIM**. Messages appears in blue.
- **Communications** - Information sent from the **SP** to the CIM. Messages appears in red.

Error Message Log

This tab displays any error messages received by the SP.

Workstations Running SP_Viewer

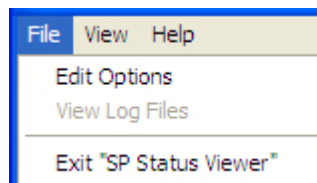


This tab is used to determine which workstation are running the SP Status viewer and allows messages to be sent to those workstations.

- **UserName** - Displays the windows user name of the workstation running View SP Status
- **PCName** - Displays the PC Name of the workstation running View SP Status
- **IPADR** - Displays the IP Address of the workstation running View SP Status
- **Broad Cast** - Sends any text entered into the field above it to all other workstation running View SP Status

SP Settings

Follow these steps to set-up the SP appropriately. When you open the **File** menu, you are presented with three selections, which are not available for users with *Read Only* privileges. They are, Edit Options, View Log File and Exit "SP Status Viewer".

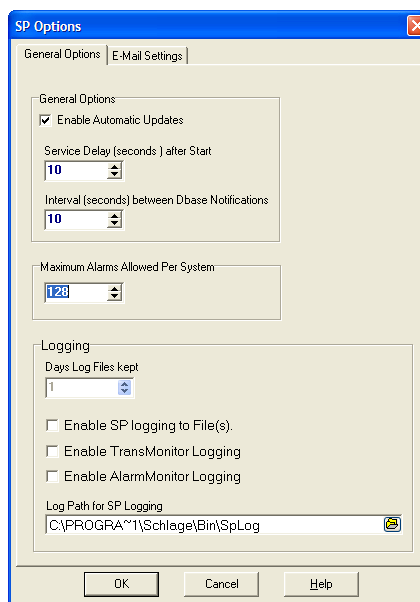


Edit options

- 1 Select this option to display the **SP Options** window that contains the **General Options** and **E-mail Settings** tabs.

General options

Within this tab there are three sections in which you need to select the appropriate settings according to your company's requirements. An illustration follows.



- 1 **Enable Automatic Updates** - Select this option to enable the SP to send a message to the CIM to update the controllers whenever there is a database change. To enable this option (enabled by default) place a check mark in the check box.

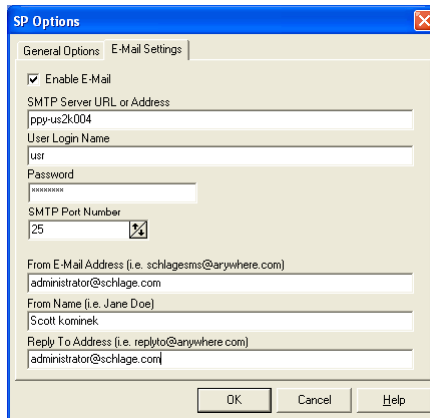
Note: The controller must also have automatic updates enabled for this to work. Please review the chapter on the CIM for details regarding controller updates.

- 2 **Service Delay** - Specify how many seconds after Start before the SP starts running.
- 3 **Interval between Dbase Notifications** - Specify how many seconds will pass between database notifications.
- 4 **Maximum Alarms Allowed Per System** - Specify the total number of alarms to be displayed in all the Alarm Monitors connected to this SP. If the maximum number is reached, the SP will acknowledge the oldest alarm to make room for the new alarm to appear. Use the up and down arrows to adjust the number of maximum alarms.
- 5 **Days Log Files Kept** - Specify the number of days of log files that are kept in the system.
- 6 **Enable SP logging to File(s)** - Must be selected for log files to be saved.
- 7 **Enable TransMonitor Logging** - Must be selected for transaction monitor log files to be saved.
- 8 **Enable AlamMonitor Logging** - Must be selected for Alarm Monitor log files to be saved.

9 Log Path for SP Logging - Define where the SP Log will be kept.

E-Mail Settings

The **System Processor** supports sending e-mail messages as alarms to designated recipients. These recipients are defined as workstations using the **System Manager** module. Please refer to that chapter for instructions on how to do this.

The image shows a screenshot of the 'SP Options' dialog box with the 'E-Mail Settings' tab selected. The dialog has a title bar with a close button. Inside, there are two tabs: 'General Options' and 'E-Mail Settings'. The 'E-Mail Settings' tab contains several fields: a checked checkbox for 'Enable E-Mail', a text field for 'SMTP Server URL or Address' with the value 'ppp-us2k004', a text field for 'User Login Name' with the value 'ust', a password field for 'Password' with masked characters, a text field for 'SMTP Port Number' with the value '25' and a small icon to its right, a text field for 'From E-Mail Address (i.e. schlagems@anywhere.com)' with the value 'administrator@schlage.com', a text field for 'From Name (i.e. Jane Doe)' with the value 'Scott Kominek', and a text field for 'Reply To Address (i.e. replyto@anywhere.com)' with the value 'administrator@schlage.com'. At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Help'.

- 1 **Enable E-Mail** - Select this option to turn on e-mailing alarms feature globally. If it is not checked, e-mail is disabled globally, regardless of any e-mail workstations entered within **Workstation Definitions (System Manager)**.
- 2 **SMTP Server URL or Address**- Enter the IP Address or URL of the SMTP Server. This host name can be any valid SMTP server with the capability of supporting standard SMTP mail formats.
- 3 **SMTP Port Number** - Enter the industry standard port number for the SMTP Server. Usually it is Port 25.
- 4 **User Login Name** - Enter the login name to the SMTP server.
- 5 **Password** - Enter the Password to the SMTP Server.
- 6 **From E-Mail Address** - The address typed here will be displayed in the 'From' area of the e-mail that is generated.
- 7 **From Name** - Enter the name that will appear on the e-mail that is generated.
- 8 **Reply To Address** - If a reply is made to the e-mail that is generated by the System Processor, the e-mail address entered here will appear automatically within the new e-mail.

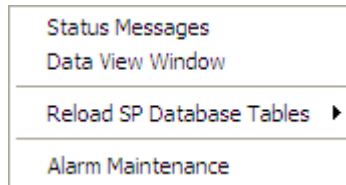
View log file

Select this option to view any SP log files that have been created. The log files are stored as text (.txt) files. These files may be reviewed using **Notepad** or any other text editor.

The SpLog file will be located in the same file as the SP_Service.exe file is located.

View menu

There are six selections in this drop down menu: Status Messages and Data View Window, Reload SP Memory, Reload Time Zones, Alarm Maintenance and Login Maintenance.



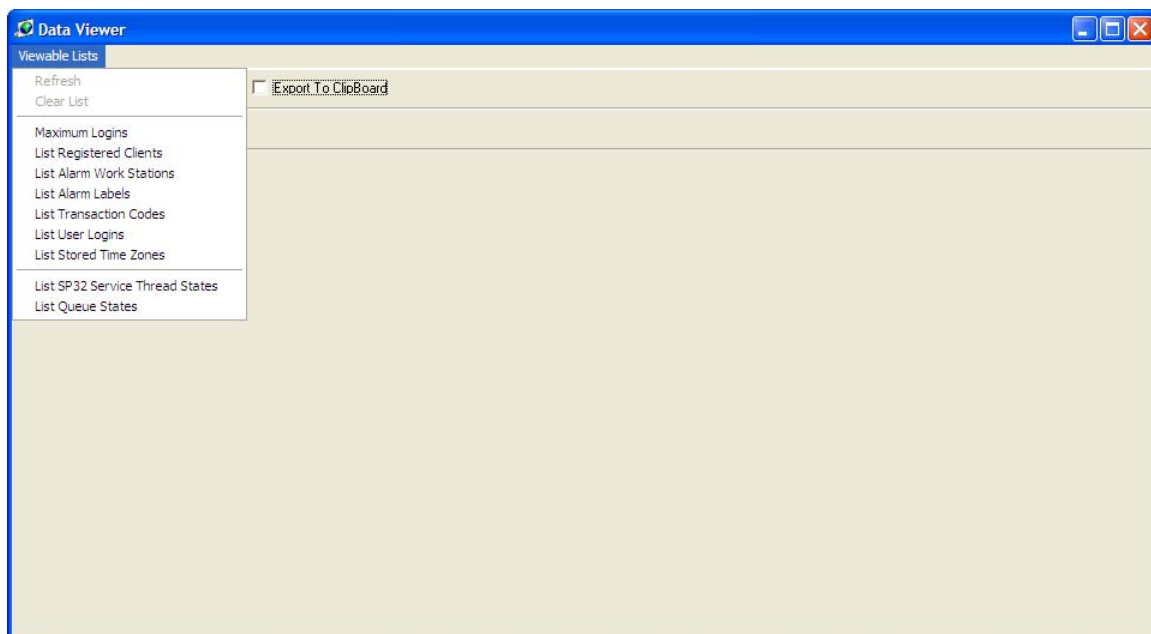
Status Messages

Select this option to open the **All Messages Log** tab.

Data view window

This selection is used for diagnostic purposes. When selecting this option the **Data Viewer** window opens showing you the list of data types that are available.

Viewable Lists

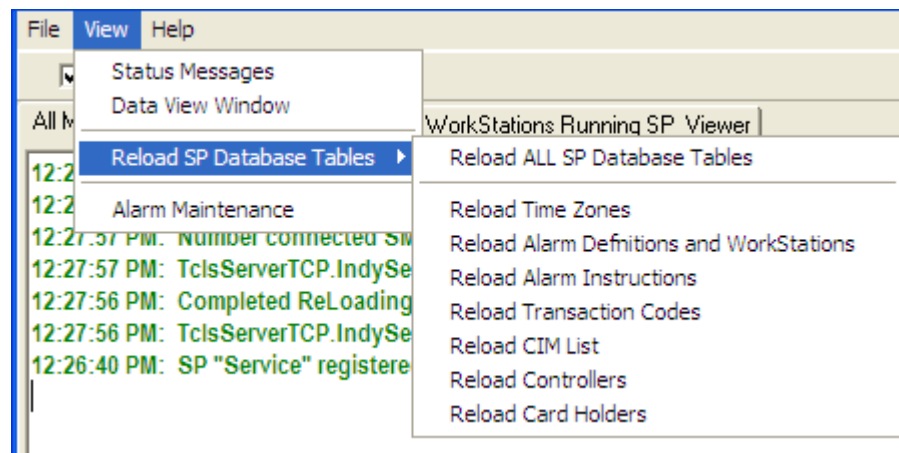


- 1 This is a sub-window of the Data Viewer. To display the list, click on Viewable Lists in the tool bar, then click on an item and the list will be displayed in Data Viewer Window.
- 2 After viewing data, if you do not click on **Clear List** the next list of data that you want to view will appear below the previous display.

- 3 **Clear List** - This option clears **Data Viewer** display
- 4 **Maximum Logins** - Displays the number of users that can be logged into the system simultaneously
- 5 **List Registered Clients** - Select this option to display the codes of clients that are connected to this SP
- 6 **List Alarm Workstations** - Select this option to view the defined Alarm Monitor Workstations or Operators presently logged in and connected to this SP.
- 7 **List Alarm Labels** - Select this option to view the codes of alarm labels from Alarm Definitions
- 8 **List Transaction Codes** - Select this option to view all the transaction codes defined by the system
- 9 **List User Logins** - Select this option to view all the users who are logged in the system
- 10 **List Stored Time Zones** - Select this option to view all the time zones defined.
- 11 **List SP32 Service Thread States** - Select this option to view all thread states of the SP Service.
- 12 **List Queue States** - Select this option to view all queue states of the SP Service.

Reload SP Database Tables

When the System Processor is launched all the information in the database (alarm, time zone information etc.) is loaded into memory. This feature deletes the selected information in the SP memory, then accesses the database and reloads the memory with the latest files. When highlighted, a series of options will be displayed.



- **Reload ALL SP Database Tables** - Deletes everything in the SP memory then replaces everything with the latest files. This includes Alarm Labels, Group Attachments, Group Names, Workstations attached to Groups, Alarm E-mail Recipients, Alarm Attachments and Time zones.
- **Reload Time Zones** - Reloads the Time Zone information only.
- **Reload Alarm Definitions and Workstations** - Reloads the Alarm Definition and Workstations information only.
- **Reload Alarm Instructions** - Reloads Alarm Instruction information only.
- **Reload Transaction Codes** - Reloads Transaction Code information only.
- **Reload CIM List** - Reloads CIM information only.
- **Reload Controllers** - Reloads controller information only.
- **Reload Card Holders** - Reloads Carholder information only.

Alarm Maintenance

The **Alarm Maintenance** feature is used for troubleshooting purposes. This window displays active and secured alarms that are currently held in the memory buffer. You can quickly view the alarm details and its transaction details.

- 1 To delete an alarm, highlight the number and transaction and use **Delete Alarm**.
- 2 To update the screen click **Refresh View**.
- 3 To close this window, select **Done**.

Exiting View SP Status Application

To exit the application select **File>Exit SP Status Viewer**. This option closes the SP Status Viewer ONLY; this does NOT shut down the SP Service.

Note: The SP Service should be running while the Schlage SMS software is running.

Controller Update

CHAPTER 38

Introduction

The **Controller update Utility** is used to update and/or reset SRCNX controller boards for changes made in the database. An expandable tree of CIM, CIM Port and Controllers is available to easily locate and identify the boards. The Communication Status window displays date, time and status of resets and updates. The operator does not need security privileges to the Communication Interface Module use this utility.

Accessing the application

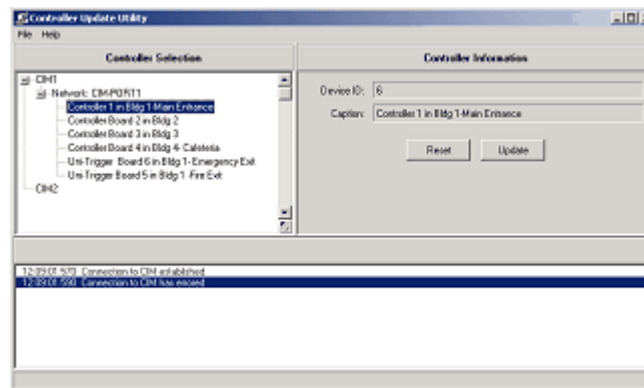
- 1 Open the **System Launcher** by double clicking on the **Schlage SMS** icon on your desktop or select **Start>Programs>Schlage SMS>Schlage SMS**.
- 2 Enter your assigned user ID and password.
- 3 In the **System Launcher** window, double click on **Downloader** icon.

Working with Controller Update Utility

Overview

The main window contains the menu bar and three sections; they are the Controller Selection, Information Display and the Communication Status Display.

A controller must be highlighted to enable File menu options. To become familiar with the different options, expand the Device Tree in the Controller Selection and observe the changes in the Information window.



Reset and Update

Following are some circumstances during which you might use either of these functions.

There is a possibility that some information on the board is corrupt; some Readers, Areas, Cardholders or Time zones did not get downloaded. By clicking on the **Reset** button, all information is downloaded to the board again.

Also, if the automatic updates feature is turned off for a particular board and you want to add the most recent changes to that board you can use the **Update** button. The Update button is also used for dial-up connections that cannot employ automatic updates.

Resetting a Controller

- 1 Select the controller from the Controller Selection section. You can expand the tree view by clicking on the plus (+) sign. The reset button becomes active on the **Controller Information** section. Click **Reset**. This will clear the controller board's time stamp to simulate the condition of having no prior updates and then download all current data to it. This option is also available in **File>Reset Selected Controller**.

Updating a controller

- 1 Select the controller by expanding the tree view. Click **Update**. All changes made in the database since the last update will be sent to the controller. The Update option will only activate when a controller is highlighted and otherwise it will be disabled. This option is also available in **File>Update Selected Controller**.

Updating a controller

- 1 If there are child boards attached to a SRCNX controller, you can update the parent and its children with a single mouse click. Select the parent controller and choose **File>Update All** Controllers.

Information section

The fields of the Information section will change depending on the device that is highlighted in the controller section. In the example below, CIM Information is shown because CIM1 was highlighted. It displays the Device ID, CIM name, Host Name and its connection status.

To review information about a CIM Port, highlight it and observe the Port Information fields. Since this example used a network port, no dial-up or baud rate is necessary.

When a controller board is highlighted, the Reset and Update buttons become available.

Communication Status Messages

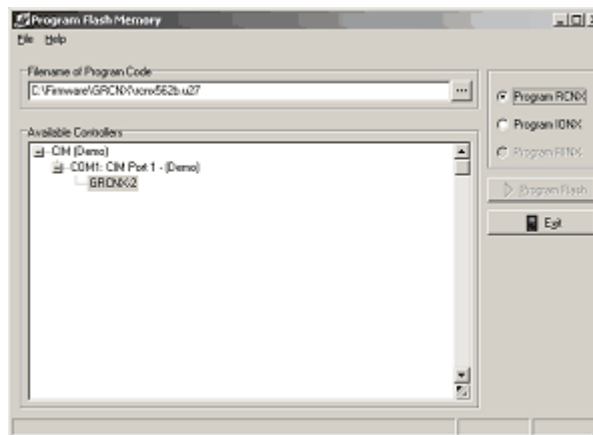
In this display window, the date, time and communication type is presented. This is also used for troubleshooting purposes since it will list the status of a Reset or Update and whether it has been successful.

Program Flash

CHAPTER 39

Introduction

The **Program Flash** module is used to download the latest firmware to SRCNX controller boards. As programs are revised to add new features and improvements, it is necessary to update the firmware.



Note: This program should not be run during the company's peak activity time such as the beginning or ending of work hours. Before this application can be used, PgmFlash.exe must be added to the Launcher tab in the System Security module. Program Flash is a control module; it is recommended that only Schlage Administrators be granted privileges to this program.

Accessing the application

- 1 Open the System Launcher by double clicking on the **Schlage SMS** icon on your desk top or select **Start>Programs>Schlage SMS>Schlage SMS**.
- 2 In the Login window, enter your user ID and password. In the **System Launcher**, select **Program Flash** icon and double click on it.

Requirements

SRCNX

- 1 **W5** - The jumper must be on to enable the EEPROM (flash chips U2 & U7) on-site program.
- 2 **W10** must have jumper on Pin 2 and Pin 3.
- 3 You must be running Version 5.x (*or higher*) of the **Schlage SMS** software.

Note: Program Flash works with the Communication Interface module (CIM) to update the firmware version on your controller boards.

Updating controller memory

Follow these steps to update the controller memory.

- 1 Simply select the path that the firmware file is stored. The firmware file type for flashing SRCNX board is U27 and for all other types of boards (SRINX, SIONX24) it is HEX.

Example C:\Firmware\RCNX

Use the browse button to locate the folder and firmware file. Highlight the file and select the open button. We recommend that you create a local folder named Firmware and copy the files into an SRCNX sub folder.

Note: When you open the Open Controller Program Code window, the Files Of Type field defaults to RC Firmware, which locates only U27 files. You should always select the Files of Type as All Files before selecting a HEX file to flash a board other than RCNX.

- 2 Click **Program RCNX or Program IONX** radio button (depending on which board you are going to update). Program RCNX is the default option.
- 3 Select the device. The **Available Controllers** section displays a list of defined controllers in your database. expand the CIM tree by clicking the plus symbol next to the CIM name to review the devices defined in your system.
- 4 Choose **Program Flash** to activate the command.

Or

- 1 Select **File>RC Source**. This opens the **Controller Download Code** window that is used to select the path where the firmware file is stored.
- 2 Highlight the board name and select **File>Program RC Flash Memory**.
- 3 This feature opens the Program Flash Memory splash screen and establishes contact with the CIM. The Access Control splash screen shows a blue progress indicator bar. The **Connection Time** window appears under the Exit button to present the actual download time in hours, minutes and seconds. An Information window will display once the upgrade is successful. This feature works the same as the Main Window Components
- 4 To close the program, use the **Exit** button.

Notes on upgrading the firmware

When upgrading firmware to a Master/Slave configuration, first send the Program Flash command to the slaves. Upgrade the master board as the last step.

Note: It is recommended that the flash not be run during peak activity time. During the time that it takes to flash the firmware, the functions of the boards will be terminated. For example, readers will not operate, contact inputs will not activate and no transactions are logged in the Transaction Monitor. Proceed with the understanding that your devices will be inactive for a short time (firmware download time plus database download time). Database download time depends on the size of the database and the number of boards to download.

You may use the Degraded Mode option to cause readers to function while you are flashing the boards. Program the readers to go into Degraded Mode *prior* to flashing the firmware. Please refer to the Readers section of the Hardware Map of System Manager chapter.

If you decide to use Degraded Mode:

The readers must be programmed to be in Degraded Mode prior to flashing. Site codes must have been previously downloaded to the boards prior to flashing.

Degraded Mode for each reader should have been checked out previously to make sure the Readers respond properly.

Note: UL has evaluated firmware 5.79 on the SRCNX.

Offline Lock Interface

CHAPTER 40

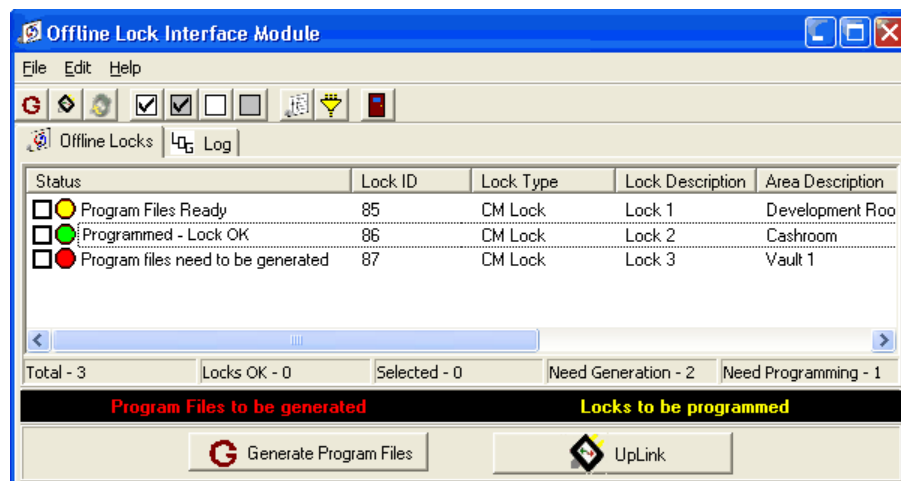
Introduction

The **Schlage SMS** requires that all offline doors are programmed when they are new, and reprogrammed as soon as the setup of a door changes. The **Offline Lock Interface** program helps to identify which doors have to be programmed, and which doors were successfully programmed. It is required and highly recommended to reprogram doors as soon as their setup is changed, otherwise settings and access rights will not be available at the door. This may cause a security risk.

When a change occurs in the database, the user is indicated with a pop up message in the system tray to receive the highest possible attention. In the main window, the status column shows a text message and a red icon that indicates which specific doors require programming.

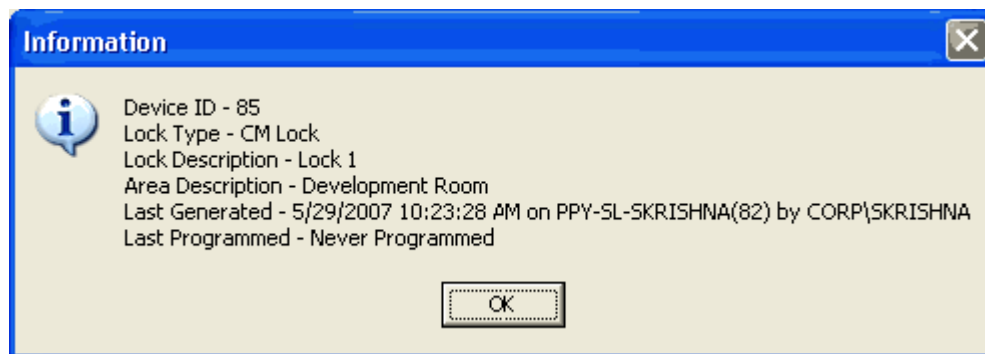
Note: Note that database connectivity is required for the Offline Lock Interface to operate. If you need to program the locks from an SMS client (i.e. a laptop) that will not have network connectivity while touring the locks, please contact technical support for assistance.

The data list is also updated when files are generated regardless of the status of the locks. Once the user clicks the **Generate Program Files** button, the program refreshes the lock information to ensure that the data is new as of half a second after the button is clicked. to ensure the data is "new" as of about a half second after clicking the button. It only refreshes at that time though. Once the program starts generating files, the data is not refreshed until the program file generation is complete.



The status column also shows the status of each lock. In the lower part of the window, you can see an overview of total number of locks, how many locks are already programmed, how many locks need to be programmed, and which locks should have new program files generated. The status is automatically refreshed at the defined interval, or users can refresh it using the **File>Refresh** option.

Users can generate program files for locks on each workstation, so that multiple workstations can generate files for the same door without interfering with each other. The **Last Generated** column shows the date and time that the programming file is generated on that particular workstation. It also shows the workstation, domain and user name where the program file is generated. This option is useful when different Windows users generate program files on a same workstation as the folder where the program file resides is different for each user. With this information, users can easily verify if the last generated file is current, and if not regenerate the file. Double click on a lock to see the following information:






Last Programmed File Date column displays the time of the file that is used to program the lock for the last time.


Note: The operator will not be able to access the locks that are attached to the areas which he/she does not have at least Read Only permissions. Those locks will not be displayed for that operator.

Working with Offline Lock Interface

Color Schemes

The following are the color Schemes used to indicate the status of the locks.

- 1  -Status unknown.
- 2  Never Programmed or Program Files Ready - Yellow indicates either the lock is never programmed or the program files have generated. Once the lock files have been generated, the next step is to synchronize those files with a PDA and program the lock.
- 3  Lock Programmed – This green icon indicates that the lock was programmed with PDA and the PDA files were synchronized back with the computer running Offline Lock Interface.

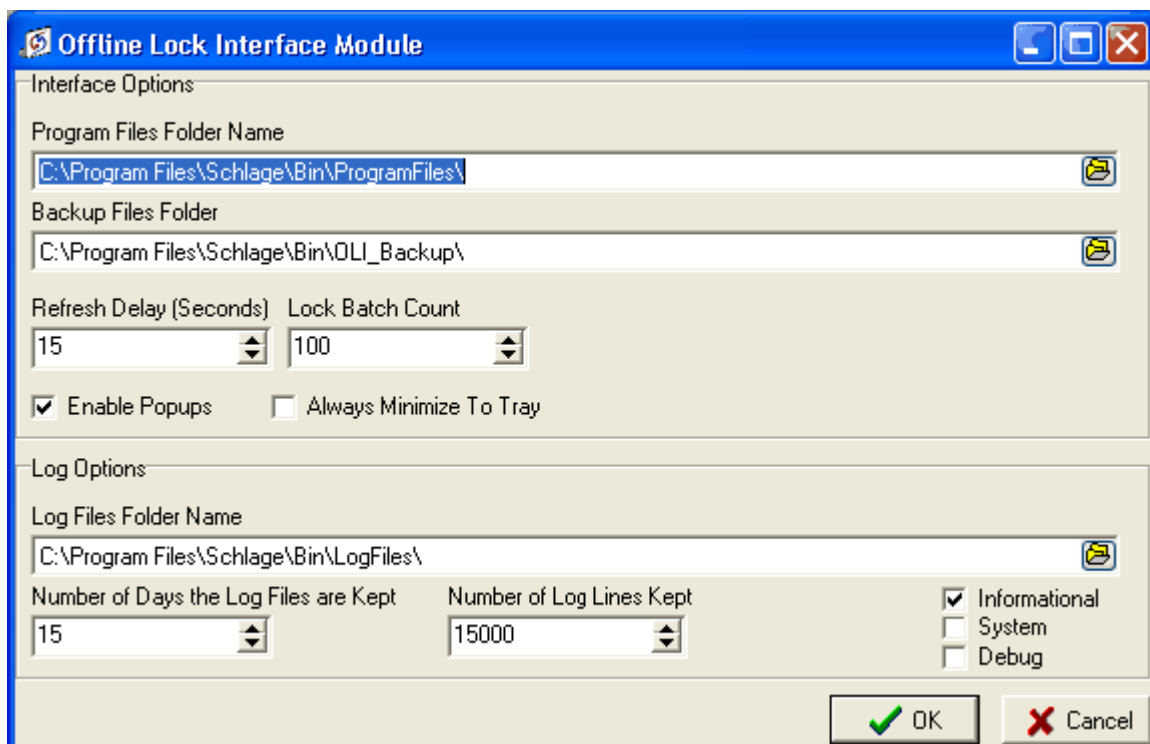
- 4  **Program Files Need to be Generated** – The locks that are in green status (programmed) can become red when there are changes to the lock description or credentials done by other access control system applications. The user is informed with a balloon message when this happens for the first time. The message does not pop up after subsequent changes are made to that lock. The locks that are in yellow status (lock files generated and lock is awaiting programming) can become red when there have been changes to the lock description or credentials done by other access control system applications. The user is informed with a balloon message when this happens for the first time. The message does not pop up after subsequent changes are made to that lock. The lock files have to be generated again, synchronized with a PDA and the lock needs to be programmed again.

Settings

Once the lock is created (in System Manager), the status of the lock is **Lock Files Never Generated**. In order to produce the log files to program the lock, the user selects the locks to be programmed and clicks on **Generate Lock Files** button.

The folder name where the files will be generated, can be found (and modified) on the Edit/ Options menu (Uplink Files Folder Name). After the lock files were generated, the status of the lock changes to yellow (Lock Files Generated).

Before generating the program files, you need to specify the export location for these files. Select **Edit>Options** to set the options for generating files.



- 1 **Program Files Folder Name** - If you are using a PDA to generate the program files, the location will be different. The system creates the files where the PDA is connected.

The folder that holds lock file should be synchronized with the PDA or the lock files needs to be transferred to the PDA into the "Uplink" directory.

Note: “Uplink” is a program on the PDA that is used to program the lock, get audit files, and to setup and configure the lock.

The PDA files (with or without audit files) have to be synchronized with the Uplink Files folder on the PC again, in order for the system to know that the particular lock was programmed. If the system finds the audit files, the audit information will be transferred to the system and the reports can be produced.

- 2 **Backup Files Folder** - Specify a folder where you want to keep the back-up version of all audit files, programming files and configuration files. If the back-up folder is not specified you will get an error message prompting you to select one.
- 3 **Refresh Delay (in seconds)** - To automatically refresh the information about the locks on the main window, set the refresh delay in seconds. The lock status will be updated based on the time that is specified here. You can also refresh the window manually by selecting **File>Refresh** option.
- 4 **Lock Batch Count** - This option allows the user to process the locks in batches when the programming files are generated. The number you enter here determines how many locks need to be included in one batch. This prevents the system from processing all the selected locks one after the other and thus creating a massive door.xml file. As the locks are broken into batches of a defined size, the system processes that many locks, creates the door files, goes back to the Program Files Need to be Generated list and picks up the next batch of locks for generation and continues the file generation until all the locks have been processed. The default value for this field is 100 (hundred). The user can adjust this value by using the up and down arrows, or by entering the value manually.
- 5 **Enable Pop-ups** - Select the check-box Enable Pop-ups. Messages pops up indicating that programming is required for specific doors when a database change occurs.
- 6 The Offline Lock Interface shows the following are the pop-up messages.
 - Audit files imported.
 - Database changes made. Locks need to be programmed.

Log options

- 1 **Enable Log** - Select this option in order for the system to create the audit file. With this option enabled, the file “YYYY_MM_DD_OLI.LOG” is created (date of the programming file generated), where YYYY= year, MM=month, DD=day. The log entries are kept for one year.
- 2 **Log Files Folder Name** - Specify the folder where the log files must be created.
- 3 **Number of Days Log Files are Kept** - Specify the number of days that the system should keep the log files. The files older than the number of days specified here are deleted. This option is only applicable to the current directory. If the user changes the directory, the system does not delete the log files that are saved in the previous one.
- 4 **Number of Log Lines Kept** - Specify the maximum number of lines that the log file should maintain in the system. The log files are automatically purged once it reaches the maximum number specified here.

Note: This option works in conjunction with the **Number of Days Log Files are Kept** option. If the maximum days set to keep the log file reaches first, the program deletes the older files regardless of the setting for Number of Log Lines Kept.

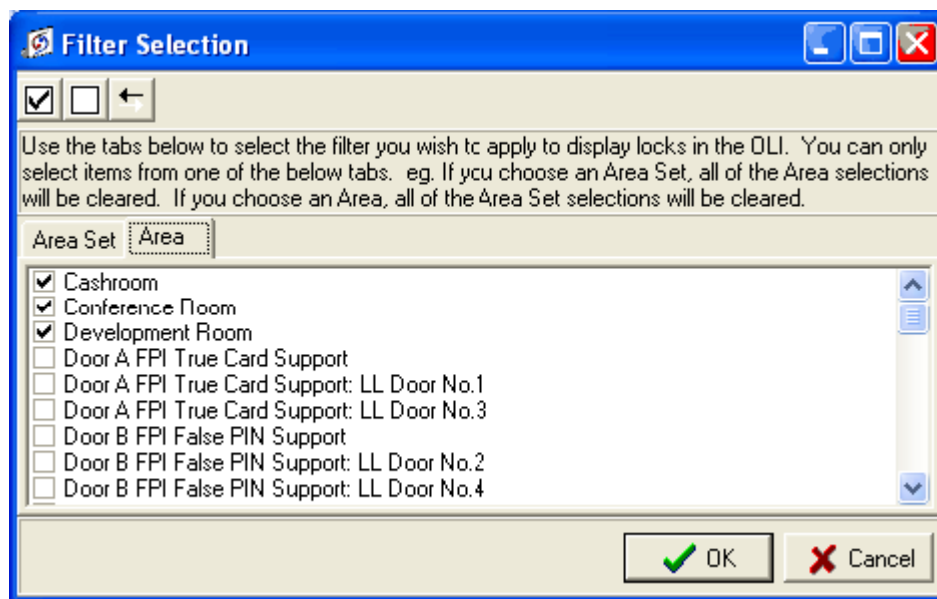
- 5 Select **OK**.

Filtering Locks by Areas or Area Set

Offline Lock Interface allows users to filter out the display of locks in the main screen based on the Area Set or Areas.



- 1 To filter the locks by Areas or Area Set, click on the toolbar icon **Set Area/Area Set filter options**.
- 2 This opens the **Filter Options** window.



- 3 Clicking on the **Area Set** tab displays the Area Sets that are defined in the system. Select the Area Sets by clicking the check box. Click **OK**. Then in the Offline Lock Interface main window, only locks that belong to the selected Area Sets are displayed.

If you click on the **Area** tab, all Areas defined in the system are displayed. Selecting the Areas causes OLI to display only locks that belong to that area.

The toolbar icons located on top of the window allows you to either select all records or unselect all records with a single mouse click.

Once the filter is active, the background color in the main window of the program is changed to Pink to notify users that the filter is active. When the filter is disabled, the background color changes to white.

Viewing log files

Follow these steps to view the log files.

Note: In order for the system to generate log files, you need to select the option Enable Log in the Lock Interface Options window.

- 1 On the main window of the program.

2 The **View Log** window opens.

- **Find this Text**- Enter the text you want to find in the adjacent field, and the system finds the first and subsequent occurrences of the text.
- **Show Lines** - If you select this option file only to the lines containing the text entered in the same edit box as for **Find This** button.
- Use **Edit>Clear Log File** option to clear the display of log files from the screen. This option does not clear the actual log file from the system, but just clears the display.

Generating programming files

- 1 Select the **Generate Program Files** button from the bottom left corner of the main window or select **File>Generate Uplink Files**. You can also use the toolbar button "Generate Program Files for checked locks".

The generated files are saved in the directory you have specified in the **Offline Lock Interface Options** window.

In order to avoid exhausting the disk space, the size of the individual logs files are limited to about 500kB. When the log file exceeds the 500kB, the file name extension is changed to "...LO1" and the subsequent audits are again being written to "...LOG" file. So, the total audit information for a particular day varies between 0 – 1M bytes in 1 or 2 log files.

Note: Now the program allows users to generate programming files on a workstation basis so that multiple workstations can generate files for the same door without interfering with each other.

Error messages

When an error is encountered, the Offline Lock Interface program prompts the user with an error message. Once the user clicks Ok, the program takes the user to the log screen so that the error can be reviewed.

Closing Offline Lock Interface

In order to get automatic notifications about the status of the locks, the Offline Lock Interface (OLI) application must run in the background (the icon should be visible on the System Tray).

If you close the program you get a message:

The message is not shown if the user closes the launcher before exiting the Offline Lock Interface application.*Programming the Locks

Note: Any reference to Ebolt is not applicable to **Schlage SMS** software.

Working with Uplink

Accessing the application

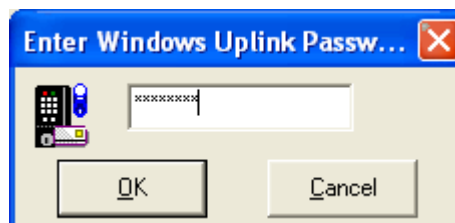
- 1 To access **Uplink**, choose **File>Launch Uplink** from the menu or select the **Launch Uplink** button at the bottom of the screen.



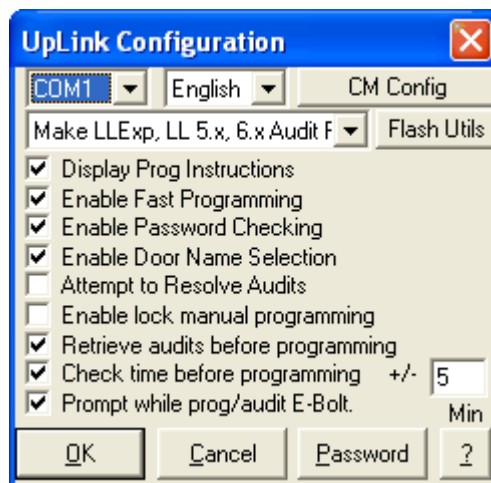
Uplink configuration

Uplink needs to be configured in order to work properly.

- 1 Click **Configuration** in the main window of Uplink and Uplink Configuration appears.
- 2 If the configuration section is password protected, **Enter Windows Uplink Password** pops up, type in the password and click **OK** to proceed, or **Cancel** or **X** to abort. Uplink Configuration is set to be password protected by default and the default password is 123456. It is recommended to change this password in order to receive the proper security.



- 3 **UpLink Configuration** has three different sections. The first section is at the top of UpLink Configuration and provides various selections and extended settings. The second section is in the middle of UpLink Configuration and offers different options on how UpLink is supposed to work. Finally, the third section at the bottom is the button bar.



Various selections and extended settings

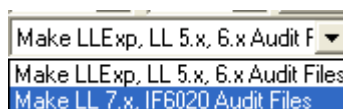
- 1 **Setting the serial port** - The first drop-down list in the top left corner is for the serial port (COM) that is used to connect the programming module. The list will only show those serial ports that are available on the system running UpLink. Click to see the list, and then click on the specific port number that is assigned to the port used for connecting the programming module.



- 2 **Selecting the UpLink user interface language** - The drop-down list next to the right specifies which language is used for the user interface of UpLink. The available languages may vary depending on the UpLink version. The default is English. Click to see the list, and then click on the specific language to use. The new language setting is activated after saving the UpLink configuration settings.



- 3 **Choosing the Audit Trail file format** - Below the top two drop-down lists is the Audit Trail file format selection. You need to select LockLink 7 audit files.



Note: A wrong selection will cause that the Schlage SMS in use cannot process the Audit Trail files although they were retrieved from the lock successfully. This can cause problems when the lock was reprogrammed after retrieving the Audits. A wrong Audit file format will cause that the Audit Trail from this Door is lost.

Follow this list for selecting the correct setting.

Software in Use Selection in UpLink Configuration

- **LockLink Express 1.x Make LLExp, LL 5.x, 6.x Audit Files**
 - **LockLink Express 2.x Make LLExp, LL 5.x, 6.x Audit Files**
 - **LockLink Express III.x Make LLExp, LL 5.x, 6.x Audit Files**
 - **LockLink 5.x Make LLExp, LL 5.x, 6.x Audit Files**
 - **LockLink 6.x Make LLExp, LL 5.x, 6.x Audit Files**
 - **LockLink 7.x Make LL 7.x, IF6020 Audit Files**
 - **InterAccess (all versions) Make LL 7.x, IF6020 Audit Files**
 - **IF 6020 with Module 650 Make LL 7.x, IF6020 Audit Files**
- 4 Click the down arrow to view the available selections. Choose the correct option by clicking on it. On the right are two buttons that open additional configuration sections within UpLink. Click **CM Config** to access **CM Lock Configuration** and **Flash Utils** for **Flash Utilities**.

Various options specifying the way UpLink works

The options in the middle section of UpLink Configuration are;

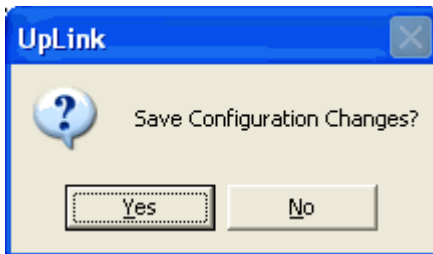
- **Display Prog Instructions** - Enables or disables the display of the **Programming Instructions** window. When this option is not checked UpLink will start downloading data to the locks as soon as Program was clicked.
- **Enable Fast Programming** - UpLink supports two data transmission speeds. Older CM locks cannot handle the fast programming speed. Whenever a problem with programming locks appears switch this option off and try again.
- **Enable Password Checking** - If there is no need to have UpLink asking for a password to enter UpLink Configuration uncheck this option.
- **Enable Door Name Selection** - If this option is switched off the UpLink user cannot select a Door name before programming. This prevents renaming Doors by accident or on purpose. The Program New Lock by Selecting Name button on **Program Lock** will be disabled.
- **Attempt to Resolve Audits** - UpLink can try to resolve the User names for the Audit Trail events. If the Audit Trail data is imported into LockLink or LockLink Express the User names do not need to be resolved by UpLink. Uncheck this box to save some amount of time when retrieving Audit Trail data from a lock. This feature is not available when LL7.x Audit Files are selected, because LL7.x Audit Files are always unresolved.
- **Retrieve Audits Before Programming** - Whenever a lock is reprogrammed all Audit Trail event entries are erased from the lock memory. To ensure that the no Audit Trail data is lost check this option to force an Audit Trail retrieval before programming.
- **Check time before programming** - This option enables checking the real time clock of the locks every time they are programmed. Enter in the field on the right of the option the allowed time frame in which the real time clock of the locks is considered to be correct. Entries are accepted for minutes only, for example entering a value of 5 means that the clock will be set if it is five or more minutes behind or five or more minutes ahead. If this option is not checked the entry for the minutes is disabled.

The button bar of UpLink Configuration

The buttons at the bottom of UpLink Configuration are **OK**, **Cancel**, **Password** and ? (help).

Saving new configuration settings

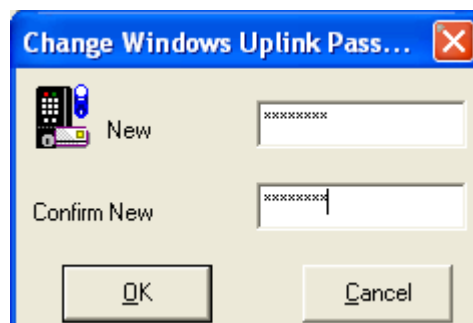
Clicking **OK** will close UpLink Configuration and display the UpLink confirmation box if changes were made. Click on Yes to save the settings, or No or **X** to discard them and have UpLink continue with the old settings.



Click on **Cancel** or **X** in the right corner of UpLink Configuration to exit directly out of the UpLink Configuration. The main window of UpLink will then be accessible again.

Changing the password for accessing UpLink Configuration

Password opens **Change Windows UpLink Password**, which is used to set a new password for opening UpLink Configuration. Type the new password into New and retype the password for confirmation in Confirm New. Click on **OK** to save the new password. To go on with the old password click Cancel or **X**. Either way Change Windows UpLink Password will close.



Accessing the Help file section for **UpLink Configuration** - Clicking on? in UpLink Configuration will show this section of the Help file.

Programming

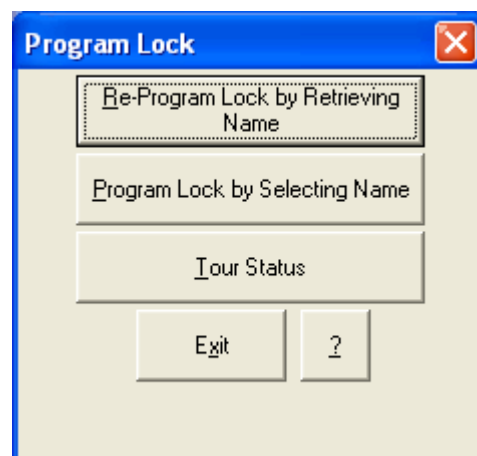
Once you have configured the Uplink program, the next step is to program the locks. Follow these steps to program locks.



The main window of **UpLink** shows the buttons **Program Lock**, **Audit Trail**, **Time/Date/ Delays**, **Utilities**, **Configuration**, **Exit**, and **About**.

Program Locks

To download program files to a lock click on **Program Lock**. This opens Program Lock and allow choosing various options. Every programming erases the Audit Trail events in a lock. If there is a need for these Audit Trail events, first retrieve the audits and then program the lock, or specify to do this procedure automatically by setting *Retrieve audits before programming* in **UpLink Configuration**.

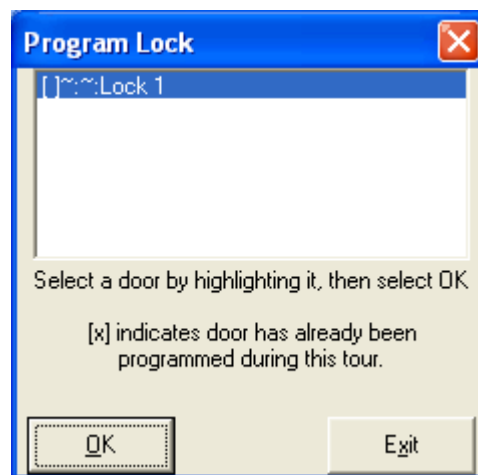


If a lock was previously programmed, UpLink can identify this lock by its name and automatically detect which program file has to be downloaded to the lock. Click on **Re-Program using the Existing Lock Name** (keyboard short cut Alt+R) to use this function. Click **Program New Lock by Selecting Name** (keyboard short cut Alt+R) when the lock was never programmed before or the door has to be renamed. Tour Status shows which Doors were programmed during the tour and which are not. To return from Program Lock to the main window of UpLink click **Exit**. For additional help on error messages see the section **Problems and Solutions with UpLink** in this chapter.

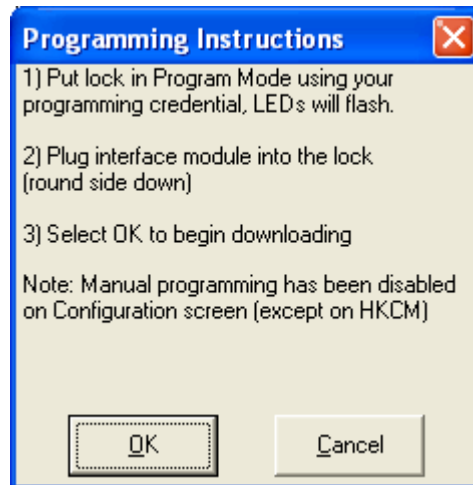
Note: Throughout UpLink and the Security Management System applications the terms “Lock” and “Door” are used interchangeably.

The programming procedure differs depending on which type of lock is programmed.

- 1 **Programming of CM Locks** - If a lock was never programmed or programming with the existing lock name fails (e. g. if the door name changed, but it is still the same physical Door), choose Program New Lock by Selecting Name from Program Lock. This specifies which program file will be downloaded to the lock.
- 2 **Re-Programming of CM Locks** - Only one door per programming procedure can be selected from the list in the door selection. Click on the door name and then click OK to proceed to Programming Instructions. Alternatively, double click on the name to proceed without clicking OK. From this point on, programming is the same as reprogramming of an already named door.
- 3 **Exit** aborts the door selection and will not download any data to the lock. Programming a lock after selecting a name will name or rename this lock. Any previous name will be overwritten and cannot be recovered without reprogramming with the proper program file. The audit trail events will be erased through programming a lock, so if there is a need for this audit information it has to be retrieved before. A [x] displayed in front of the door name indicates that this door was previously programmed during the current tour.



- 4 When Programming Instructions appears insert the programming key into the programming module and click **OK**. Data will be transferred to programming key. Some windows will appear quickly and the change from one window to the next is only received as a quick flashing, which is normal. Click **Cancel** to exit at this point without programming.

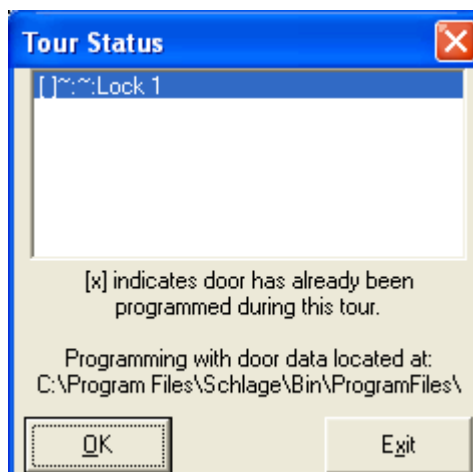


Reprogramming using the Programming Key and detecting the existing Door Name/Retrieving Audits before reprogramming

When the CM Lock was previously programmed it has already a name, so there is no need to select the name before reprogramming, unless a new name has to be assigned. Select **Re-Program using the Existing Lock Name** in order to automatically retrieve the door name from the CM Lock. Only this method will also retrieve audits before programming if the option Retrieve audits before programming is selected in UpLink Configuration.

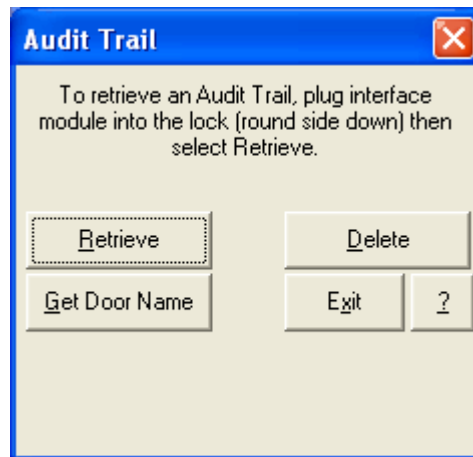
The procedure for data exchange between programming module and CM Lock by using the Programming key is the same as for programming with assigning a new Door name.

- 5 **Viewing the Tour Status** - Click on Tour Status in Program Lock to see an overview of which door is already programmed and which not. A list will appear and all those doors that are already programmed during the current tour will have an [x] in front the door name, all others will have an [] only. To close Tour Status click OK or Exit, or X in the upper right corner of the window, or double click in the list box. Tour Status is only used to display information; no data is processed.



Audit trail

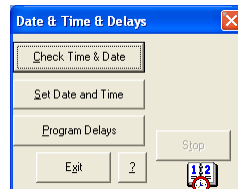
The locks with the ATR or SMT feature, and the E-Bolt deadbolt store Audit Trail events. To work with these Audit Trail events click on Audit Trail in the main window. This will display **Audit Trail**.



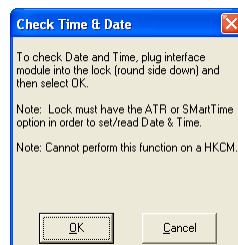
- 1 When retrieving audit trail data from an CM Lock using the Programming Key, follow this link to the description of **Retrieving Audit Trail Data from an CM Lock**. Otherwise follow the instructions below. For additional help on error messages see the section **Problems and Solutions with UpLink** in this chapter.
- 2 Make sure that the interface module is plugged into the lock correctly to load audit trail events from the lock and then click on **Retrieve**. The upload process will start immediately. No event will be altered or erased when retrieving Audit Trail data, only programming erases all events. Press the Esc key on the keyboard to stop the upload process. All Audit Trail events are stored in a file that is processed by the Access Control Management System application at a later point. If there is an old audit trail file already available UpLink will prompt if this file can be overwritten.
- 3 Click on **Yes** to overwrite with the new file or click **No** to cancel the operation and have nothing changed or erased.
- 4 Delete on Audit Trail allows deleting any Audit Trail file created by UpLink in the current file location. Select the Door name for which the Audit Trail file should be erased and click **OK** to proceed, or click **Exit** or to cancel and delete no files.
- 5 After clicking **No** to cancel. Either decision will return to Audit Trail. The delete function works only when Audit Trail files are available, otherwise an error message appears.
- 6 Click **Exit** on **Audit Trail** to close this window and have the main window of UpLink be accessible again.

Date & Time Delays

Date & Time & Delays provides tools for setting the real time clock of SmartTime locks and defining the different door delays for relock, nuisance, and door prop.

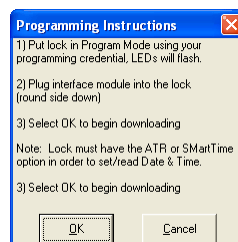
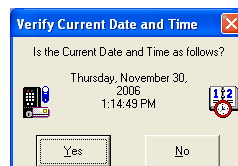


- 1 Click **Check Time & Date** to read out the real time clock of the lock. **Check Time & Date** appears. Only locks with ATR or SmartTime option have a real time clock.
- 2 Click **OK** to proceed, or up **Cancel** or to return to **Date & Time & Delays**.

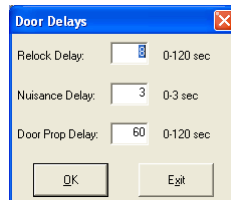


- 3 Make sure that the interface module is properly plugged into the lock. Reading the time and date from the lock is not only to verify if time and date is current in the lock, but is also a basic communication test between UpLink and the lock. Stop in **Date & Time & Delays** ends reading time and date from the real time clock.

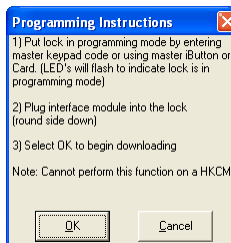
If checking time and date shows that the clock in the lock is not running with the correct time then click on **Set Date and Time** in Date & Time & Delays to synchronize the clock on the lock with the clock of the computer running UpLink. The time in the clock is only as accurate as the computer it is programmed with. To ensure that time and date are always accurate set check time before programming in **UpLink Configuration** to have date and time checked every time a door is programmed. Click **Yes** in **Verify Current Date and Time** if time and date are correct, or choose **No** to cancel. Then set the system clock of the computer running UpLink to the correct time and date. The master programming credential is needed to set time and date, and the interface module has to be plugged in. Programming Instructions will give step-by-step advice.



- 4 UpLink can be used to program the door delays. Click **Program Delays** in Date & Time & Delays and set the delays to the desired values. The delay times are displayed right next to Relock Delay, Nuisance Delay, and Door Prop Delay. All delays are measured in seconds. The fields will show the default values if Door Delays is opened. Click **Exit** to return to Date & Time & Delays.



- 5 Click **OK** to program the delays and follow the steps shown in Programming Instructions. Click **Cancel** or **X** to discard the entered delay times and to return to Date & Time & Delays.



Closing Date and Time Delays and accessing the Help file

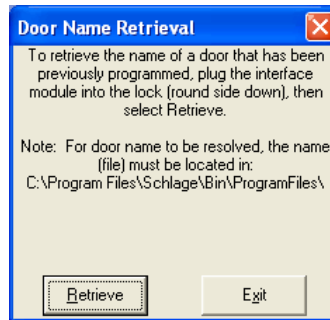
Exit or **X** on **Date & Time & Delays** closes this window and shows the main window of UpLink again. Click **?** to see this section of the Help file. For additional help on error messages see the section **Problems and Solutions with UpLink** in this chapter.

Utilities

Utilities provides two functions. The first one is **Retrieve Door Name** and the second one is **Enroll Using Hand Reader**. Click **Exit** or **X** to close Utilities and return to the main window.



UpLink can retrieve the door name from the lock memory. Click **Retrieve Door Name** in Utilities. Door Name Retrieval appears and will give brief instructions on how to retrieve the name. Plug the interface module into the lock and click **Retrieve**. UpLink will read out the name and display it in the bottom of Door Name Retrieval. To get back to the main window of UpLink click on **Exit** or in **Door Name Retrieval** and **Utilities**.



How to resolve problems with UpLink

There are some common problems that may arise while using UpLink. The following points have to assured to give UpLink a chance to work properly:

- 1 The programming interface has to be properly connected to the programming cable, which needs to be properly plugged into the programming device.
- 2 The programming interface has to be plugged into the lock correctly (round side down for CIP).
- 3 The programming credential has to be used prior to programming.
- 4 With this UpLink can program a door and receive audit trails (no programming credential needed to receive audit information). Still there may be some error messages come up. If the errors persist do the following:
- 5 Check the configuration settings
- 6 Try changing the programming module
- 7 Check the programming cable (has to be special serial cable, a regular cable does not work)
- 8 Check if the batteries in a stand-alone lock provide enough power
- 9 Check if the batteries in the programming device are properly charged.

All error messages close by clicking OK or **X**, unless stated otherwise. The following error messages are described in detail:

Error messages

1 Too Many Sync Tries

The programming device cannot establish a communication with the lock. This error can be caused by a number of reasons. First try turning off any other applications that are running (except the access control management software) and try the operation that raised the error again, if that does not work try the following:

In the main window of UpLink click on **Utilities**, then select **Retrieve Door Name** and follow the instructions on the Door Name Retrieval window.

If you still get the 'Too Many Sync Retries' error the cause is one of the following (check each one, and try to retrieve the door name again after any change made):

- a) The CIP programming module may be installed incorrectly
 - Make sure it is plugged in round side down.
 - Make sure it is connected to the cable end labeled RDR.
 - b) The COM Port setting is wrong or some other application (such as palmtop syncing software or infrared communication) has priority over the COM port.
 - Verify the COM port settings in the UpLink Configuration.
 - Close any applications that may be using the COM port
 - Turn off the IR port if it is turned on (you may have to go to the computer's Control Panel / Settings)
 - c) The Fast Programming Mode is selected and causing a conflict. Deselect Fast Programming from the **UpLink Configuration**.
 - d) The serial cable and / or CIP module may be defective. Try swapping each one.
 - e) If the 'Too Many Sync Retries' error does not appear when retrieving the door name the communication between the lock and the programming device is working properly. The cause is one of the following (check each one, and try the original action that caused the error after any change made):
 - f) The lock has not been put in programming mode before trying to program the lock. The on-screen instructions state to put the lock in programming mode by using a Programming Credential before plugging the cable in ROUND side down and then clicking OK. If the lock was in programming mode and there was no data transfer initiated within 30 seconds the lock will return to normal operation mode. Reuse the programming credential and try again.
 - g) Enable Time Check Before Programming or Enable Audit Trail Before Programming are selected on UpLink Configuration, and there is no ATR or SMT option installed on the lock. Deselect Enable Time Check Before Programming and Enable Audit Trail Before Programming on **UpLink Configuration** if the lock does not have the ATR or SMT option.
 - h) The Fast Programming Mode is selected and causing a conflict. Deselect Enable Fast Programming from **UpLink Configuration**.
- 2 Error - No exported data found**
- UpLink cannot find any program files that can be used for programming doors. Export the door files again and/or make sure that they reside in the same folder as UpLink.
- 3 Lock has not been named yet**
- The lock is programmed for the first time or the available program files do not match this lock. Choose Program New Lock by Selecting Name from the **Program Lock** window and give the lock a new name by specifying the correct door file.
- 4 Error - Too much time between incoming characters**
- The connection between cable, programming interface and lock is bad. Check if the interface is plugged correctly into the lock, if it was not unplugged during programming or audit retrieval or if any other reason causes a bad connection such as dirt, dust, moisture etc. If this error appears during programming switch of the fast programming mode in the **UpLink Configuration**.
- 5 Door Programming Warning**
- If a door was already programmed during a tour and it is tried to program this door again a warning comes up. Reprogramming a door with the same programming file will affect the audit trail, because any events that occurred during the first programming and reprogramming will be lost. It is not recommended to reprogram a lock during the same tour if there is no reason requiring a reprogramming. Click **OK** to proceed, or Cancel or **X** to abort.
- 6 Error Opening Communications Port**

The COM port (serial port) setting is wrong or some other application (such as palmtop synchronization software or infrared communication) has priority over the COM port. To resolve this problem verify the COM port setting from the **UpLink Configuration** screen, close any applications that may be using the COM port, turn off the IR port (may have to go to the computers Control Panel / Settings).

7 Too Many Repeated Pages

The communication quality between programming device and lock is poor and the received data has errors. A possible solution is to check all connections of the serial cable and the programming interface.

8 Previous Audit Report Exists, Overwrite?

After retrieving an audit from a lock UpLink stores the audit trail events in a file. If there is an older audit file already existing UpLink will ask if this file can be overwritten. Click Yes if this audit file was already resolved by the Access Control Management Software (can be displayed as Audit) or **No** if it was not resolved or if you are not sure. Close UpLink and resolve the audit with the management software.

9 Error Getting Communications Port State

This error appears if any other hard- or software is interfering with the serial communication port, UpLink may get stuck in a loop repeating this message. Press the Enter key and immediately afterwards the Esc key to abort this procedure. More than one try may be necessary.

10 Cancelled By User

A procedure was cancelled by the System Operator using UpLink, for example by pressing the Esc key on the keyboard.

Working With Schlage Utility Software (SUS)

The Schlage Utility Software (SUS) is used to program the new AD Series offline locks. SUS runs on the Pidion PDA that is included with the offline locks. For Windows XP, ActiveSync needs to be installed on the PC. For Windows Vista, Windows Mobile Device needs to be installed on the PC.

Once the appropriate sync program is installed, program files can easily be downloaded to the PDA and uploaded to the lock, and audit files can be downloaded from the lock and uploaded to SMS. See the **Schlage Utility Software Manual** for details.

Sync Program Configuration

For Windows XP, ActiveSync needs to be installed on the PC. For Windows Vista, Windows Mobile Device needs to be installed on the PC. Follow the directions below to download and set up the sync program and to configure the OLI application.

Download Sync Program

For Windows XP:

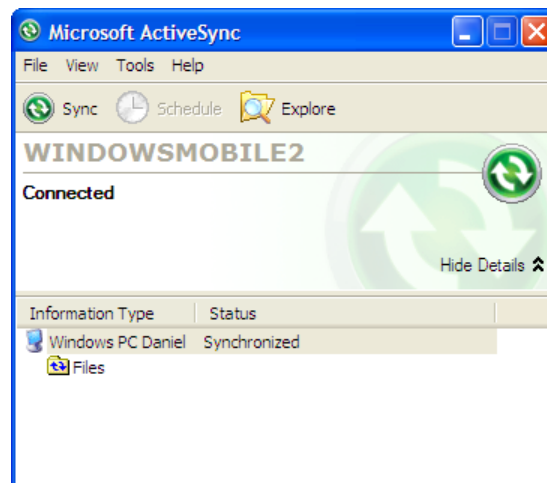
- 1 Go to www.microsoft.com.
- 2 Search for "ActiveSync".
- 3 Select the "information and downloads" option from the search results.
- 4 Follow the instructions provided to download the ActiveSynch installer.
- 5 Once the installer is downloaded, run the program. Follow the instructions provided to install ActiveSynch.

For Windows Vista:

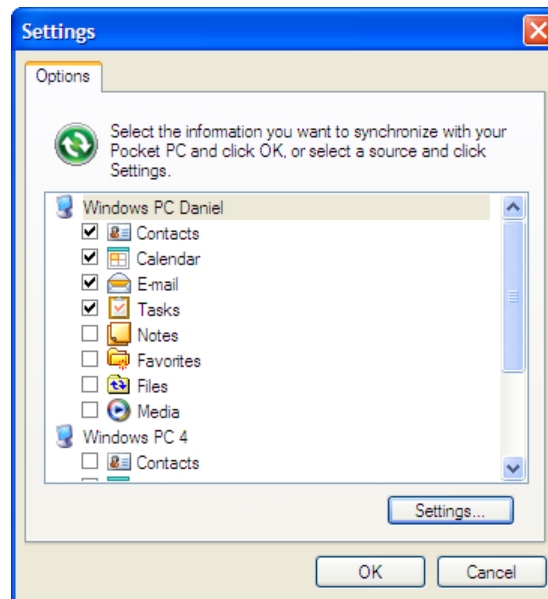
- 1 Go to www.microsoft.com.
- 2 Search for "Windows Mobile Device Center".
- 3 Select the "download details" option from the search results.
- 4 Follow the instructions provided to download the Windows Mobile Device Center installer.
- 5 Once the installer is downloaded, run the program. Follow the instructions provided to install Windows Mobile Device Center.

Set Up Sync Program

- 1 Once the sync program has been downloaded and installed it should be configured.
- 2 Connect the PDA to the computer using the USB cable.
- 3 ActiveSync will start automatically. It will take a moment for it to connect to the PDA.



- 4 Go to **File>Options**. The **Settings** window will open.

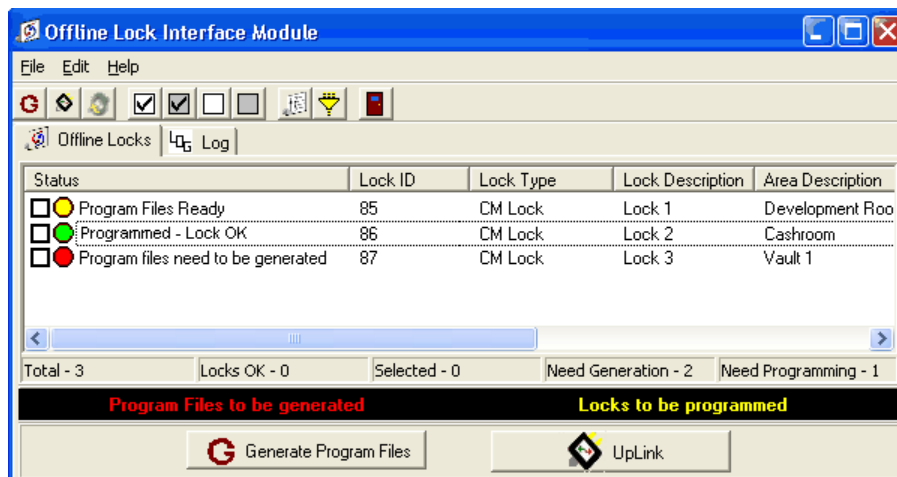


- 5 Remove all check marks by clicking on any option that has a check mark in it.
- 6 Add a check mark to the **Files** option by clicking on it. A **File Synchronization** window will open.
 - a) Click **OK**. The File Synchronization window will close and a check will be put into the Files option.
- 7 Click **OK**. The Settings window will close and ActiveSync will re-connect with the PC.
 - A new folder will be added to the **My Documents** section of the PC. This folder will hold the Program Files for the offline locks. The folder name will be either **ActiveSync My Documents** or **WindowsMobile My Documents** depending on if this is installed on Windows XP or Windows Vista, respectively.

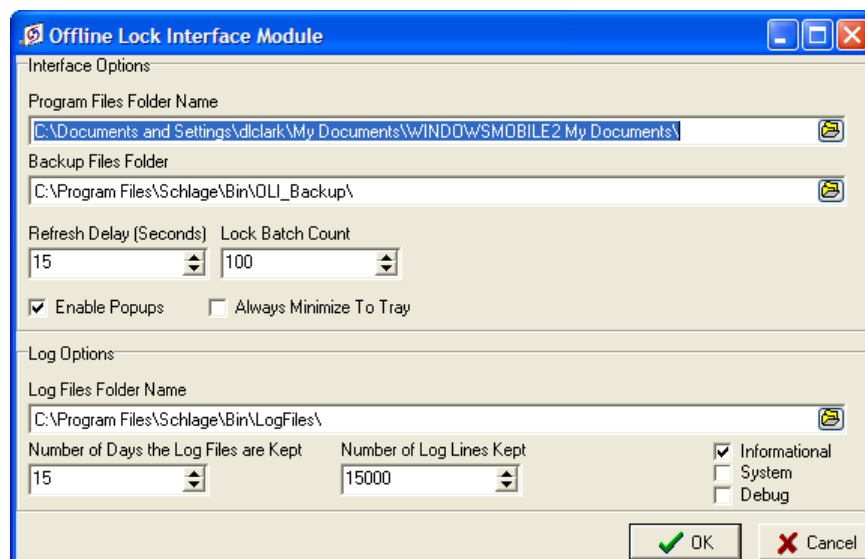
Configure OLI to work with Windows Sync Application

- 1 Once the sync application has been downloaded, installed, and configured, the new Program Files location must be entered into the Offline Lock Interface application.

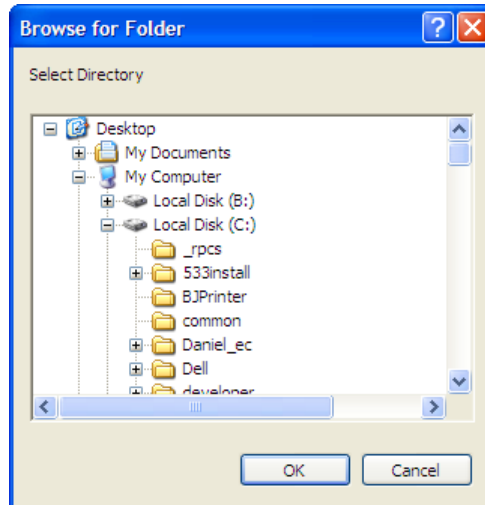
- 2 Open the OLI application.



- 3 Go to **Edit>Options**.



- Click on the **Explore** button to the right of the **Program Files Folder Name** field. The **Browse for Folder** window will open.



- Find and select the folder created by ActiveSync to hold the Program Files. Example: **C:\Documents and Settings\dlclark\My Documents\WINDOWSMOBILE My Documents**
- Click **OK**. The Browse for Folder window will close and the selected folder will populate the Program Files Folder Name field.
- Click **OK**. The options window will close and the OLI application will be ready to generate program files.

Program Lock

Once the sync program has been installed and configured, the SUS can be used to program a lock.

Update the program files on the PDA

- Go to the OLI.
- Select the locks to be programed.
- Click on the **Generate Program Files** button.
- Once the files have been generated, connect the PDA to the PC running the OLI. The ActiveSynch program will start automatically on the PC.

NOTE: The SUS can not be running when the PDA is connected to the PC. If it is, the ActiveSynch program will not start.

- Once the files have been synchronized, disconnect the PDA from the PC.

Program a lock for the first time:

- Update the files on the PDA. See the above section for details.
- Connect the PDA to the offline lock to be programed.
- Click **Start** on the PDA. A Menu will open with a list of programs.

- 4 Select the **Schlage Utility Software** option. **SUS** will open.
- 5 Select **Manager** from the **Log on as** drop down menu.
- 6 Enter the password into the **Password** field. Default password is **123456**
- 7 Click the **Login** button. The SUS program will open. The locks with program files will be listed in the top screen and the bottom of the screen will say **No Device Connected**.
- 8 Put the AD Series lock into program mode:
 - a) Press the **Schlage** button on the AD keypad twice. Red LEDs will flash.
 - b) Enter **97531*** on the AD keypad. The Red LEDs will flash rapidly for a moment. The lock is in Program Mode. The bottom of the SUS screen will say **No Door data available**.
- 9 Click on **Options** at the bottom of the screen. A list of options will open.
- 10 Click on the **Setup Lock** option. All the doors that have had program files uploaded to the PDA will appear in a list.
- 11 Select which door file to download to the lock.
- 12 Click **Ok**.
- 13 The lock's date and time will update, then the lock will be set up. Wait while the lock is set up. The SUS will display when it is finished and the set up window will close and the options list will be presented.
- 14 Click on **Back**. The options list will close and the SUS main screen will open. The newly programmed lock will appear at the bottom of the screen while the locks to be programmed will be listed at the top.
- 15 Double click the currently connected lock at the bottom of the screen. The **Collecting Audit** window will open. It will close when the Audit has finished uploading to the PDA.
- 16 This lock is programmed. Disconnect the PDA and repeat the steps above for each new AD lock to be programmed.

Update a lock

- 1 Update the files on the PDA. See the above section for details.
- 2 Connect the PDA to the offline lock to be programmed.
- 3 Click **Start** on the PDA. A Menu will open with a list of programs.
- 4 Select the **Schlage Utility Software** option. **SUS** will open.
- 5 Select **Manager** from the Log on as drop down menu.
- 6 Enter the password into the **Password** field. Default password is **123456**
- 7 Click the **Login** button. The SUS program will open. The locks with program files will be listed in the top screen and the bottom of the screen will say No Device Connected.
- 8 Put the AD Series lock into program mode:
 - a) Press the **Schlage** button on the AD keypad twice. Red LEDs will flash.
 - b) Enter **97531*** on the AD keypad. The Red LEDs will flash rapidly for a moment. The lock is in Program Mode. The bottom of the SUS screen will now display the name of the connected lock.
- 9 Double click the connected lock. The **Collecting Audit** window will open. It will close when the Audit has finished uploading to the PDA.

- 10 The lock has been updated.

Update the SMS files

- 1 After the Audit has been downloaded from the lock to the PDA, disconnect the PDA from the lock.
- 2 Click on **ok** at the top right of the SUS window. This will close the SUS program.
- 3 Connect the PDA to the PC running the OLI.
- 4 ActiveSync will start automatically. The files will be updated. All lock audit files that were uploaded to the PDA will be downloaded to SMS and the OLI will reflect that those locks have been programmed.

Campus Locks

CHAPTER 41

Introduction

The **Schlage SMS Campus Lock System** provides a security solution for college campuses. This offline locking system gives you flexibility, scalability, and quality needed to manage the security and access control requirements of the large student and faculty population in campuses around the world. Integrated with **Schlage SMS**, the Campus Lock System is managed using the same user interface of the online system.

Configuration

Overview

The configuration of Campus Lock System involves, defining an access plan, definition of user types, and definition of campus locks. The Campus lock reader does not directly communicate with the host controller. So it is necessary to do manual programming at the reader location. The user can create necessary downloadable files and upload to a pocket PC or laptop using a serial port or the USB port of the AD-250 Series. The data is transferred by connecting to the serial communication port of the PC or to the USB port for AD-250 Series. The files required for programming the locks are generated to a folder using the **Offline Lock Interface Module**. The programming of doors is accomplished by connecting a **CIP** (Computer Interface PAK) from the laptop/palmtop to the iButton ports of the lock.

Once the access plan has been created and locks properly set up, the user can then create campus lock credentials for cardholders using the Cardholder Definition program. Once the credentials are defined properly, the data is encoded to the mag card using the Magstripe encoder.

The Campus lock system comes with the following features that cater to the special security needs of college campuses:

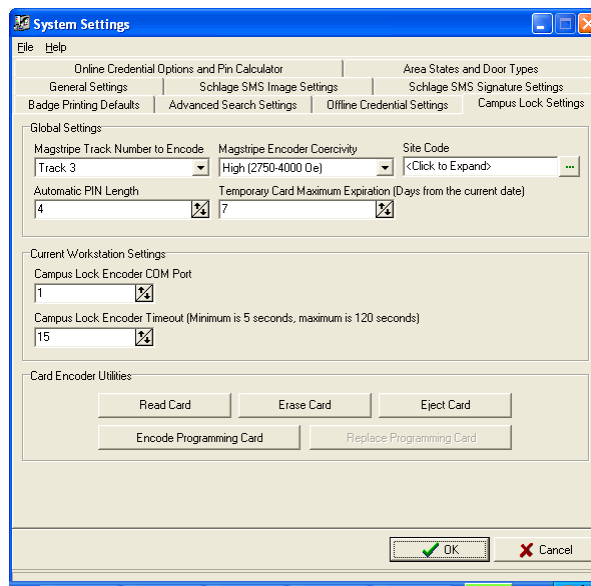
- 1 The **Access Plan Definition** program allows the user to define the access templates in a hierarchical way. This feature allows the creation of plans that may contain one or more buildings, buildings may contain one or more floors, and floors could have one or more rooms.
- 2 The access plan is customizable which allows the user to use their own nomenclature to name properties of their access plan.
- 3 The lock definition feature has the option for gender selection to restrict access based on gender. It also allows ADA specific timing.
- 4 Providing access based on user types defined in the system adds another level of security.
- 5 Lock and the system software is capable of accommodating unlimited number of key cards and unique PIN codes.
- 6 Manages an unlimited number of PIN codes where card and PIN is required for access.

- 7 The Cardholder definition program of the application has the new 'key selection option' that allows the user to have access to separate buildings using separate keys. One key could be defined to expire after a period of time.
- 8 Campus Locks support first person in functionality. Programming an automatic override for a specific lock and selecting the option "Credential Enabled" allows the user to activate an automatic override only by a valid access.
- 9 The campus lock credential can be saved and encoded on to the card using the Magstripe encoder hardware within the campus lock credential definition dialog.

Campus Lock Settings

Follow these steps to specify the campus lock settings. These settings need to be specified properly in order to encode a campus mag card.

- 1 Open the **System Settings** module.
- 2 Select the tab **Campus Lock Settings**.



- 3 The first section is the global section. These settings are global throughout the system, and can only be changed by an operator with administrative rights to **System Settings**.
 - a) **Magstripe Track Number to Encode** - This is the track number of the Magstripe cards that the system will use while encoding a card. Track 3 is the standard track number to encode.
 - b) **Magstripe Encoder Coercivity** - The three options in this combo box are High, Medium, and Low with High being the default. This option must match the Magstripe badges the customer buys otherwise it will not encode properly and may damage the cards.

Low coercivity - As the name implies, low field energy is used to write data onto the magnetic stripe of an ID card designed for low-energy encoding. Low-coercivity encoded cards are best used for medium-use, non-critical, security applications. One of the main benefits of using low-coercivity cards is the low cost.

High coercivity - High-coercivity uses strong magnetic field energy to write data onto the magnetic stripe of an ID card designed for high-energy encoding. High-coercivity encoded cards are best used in high-usage environments such as secured installations, where the long-life of the data on the magnetic stripe is of extreme importance. High-coercivity cards are resistant to data loss due to the high level of energy used to encode them. It is important to use the appropriate encoder-type printer with the appropriate coercivity cards. For example, if you use a low-coercivity encoder printer with high-coercivity cards, the field intensity created by the encoder will not be enough to permanently polarize the receptive material of the card. The magnetic stripe will rapidly lose its encoded information.

In the opposite case, in which a high-coercivity encoder is used with low-coercivity cards, the magnetic field created by the encoder will saturate the magnetic stripe of the card, rendering it useless, and the printer will not be able to verify the card.

- 4 **Temporary Card Maximum Range (Days from the current date)** – This setting is used within the Cardholder Definitions module when an operator wants to create a temporary campus lock credential for a cardholder. If this is set to 7, then the temporary card is valid up to 7 days from the date of issue. The minimum is 1 day and the maximum is 31 days.
- 5 **Current Workstation Settings** - The settings under this section will only take effect on the current workstation. These can be changed by operators who have Read/write permissions to System Settings application.
 - a) **Campus Lock Encoder COM Port** – The COM Port the encoder is connected to. This only applies to workstations that have an encoder connected. Valid values are 1 to 255.
 - b) **Campus Lock Encoder Time-out** - This is the amount of seconds it will take the encoder to time-out while waiting for a card to be placed into it. Valid values are 5 to 120 seconds.
 - c) **Card Encoder Utilities** - The next section has four different functions you can perform with the **Card Encoder**.
 - **Encode Programming Card** - This option is used to encode a "master" programming card. "Master" Programming card allows users to put a campus lock in programming mode. Only operators with administrator permissions to this application can perform this operation.
 - **Read Card** - This option allows users to read the track that the system is using from a card that is placed into the encoder. The data will be displayed in XML format. Only operators with administrator permissions to this application can perform this operation.
 - **Erase Card** – Clicking this option completely erases a card that is placed into the encoder. It will erase all the tracks of the card. Only operators with administrator permissions to this application can perform this operation.
 - **Eject Card** – Click this option to remove a card from the encoder.

Instruction to Register a Programming Credential

For a legacy CL lock, follow the instructions below.

- 1 Open the back of the lock.
- 2 On the electronics board, press and release the **INI** button THREE times. The red LED will light and remain on.
- 3 Present the "master" credential to the reader. The green and red LEDs will alternately flash indicating acceptance.

For an AD250 CL lock, follow the instructions below.

- 1 Remove the lock's inside cover.

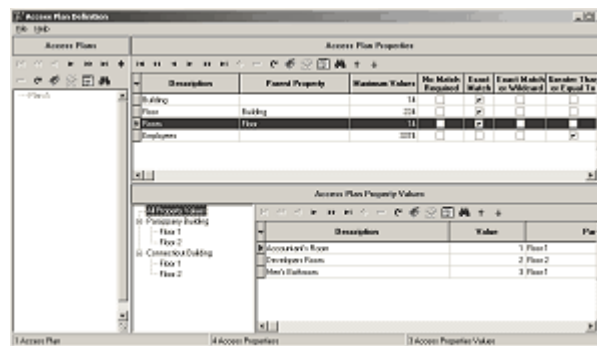
- 2 While pressing the **Inside Push Button**, press and release the **Tamper Switch** 3 times within 5 seconds. The **IPB** red led and left red Schlage LED will turn on.
- 3 Insert and remove a "master" magnetic stripe card into the lock. The IPB red LED and left Schlage red LED will turn off. The Schlage LEDs will toggle green / red 5 times to indicate acceptance of the master card.

Note: If the card was not a master credential, or was not read correctly, then the Schlage Red LEDs will flash 2 times, signifying that the master credential was not changed.

After manually programming the master credential, any previous master credential Card or default master PIN is deleted from the lock.

Defining Access Plans for Campus Locks

In the Campus lock system, the access plans are defined using the **Access Definition Module**. This module allows the user to define an access plan, various properties, and appropriate property values for a Campus lock.



The Access Definition Module has three sections. The left hand side of the section contains access plans in a tree view in alphabetical order. Sorting is not allowed in this pane. The upper section shows all properties defined in the selected plan, and the bottom section contains the property values. All grids support the Export to File pop-up menu option.

Note: If the user has read only permissions to the application, the insert, delete, move up, and move down buttons will not be active.

Adding an Access Plan

Follow these steps to define an access plan.

- 1 Open the **Access Plan Definition** Module.
- 2 Select the **Insert (+)** button from the top left pane of the main window.
- 3 The **Access Plan Definition** window opens. Enter a description and the notes attached to it.
- 4 Select **Save and Close** to save the record. Select **Save and New** to save the current record and add a new one. Click **Close** to exit the window without saving the record.

A maximum of fourteen (14) access plans can be defined in the system. Once the maximum number is reached, the insert button is disabled. The access plans are also disabled if the permission is currently set to read only. Only operator's with administrator rights can modify or delete access plans that are Read only. If changes are made to a locked access plan, all existing campus locks may need to be re-programmed and Magstripe cards may need to be re-encoded. This includes their properties and property values. There are a few different situations that would make an access plan grayed out:

- a) The application is set to read only in the Launcher program.
- b) A campus lock is defined in System Manager and is currently using the access plan.
- c) A campus lock credential is defined and is currently using the access plan for one of its card access values.

Editing an Access Plan

- 1 Double click on the record to open the **Access Plan Definition** window. Make the required modifications and click **Save and Close**.

Deleting an Access Plan

- 1 Select the access plan you want to delete, and choose the delete (-) button.

Note: The user needs at least read/write permissions to an access plan to delete it.

Defining Access Plan Properties

The access plan property pane is on the right top part of the main form. The grid displays all the access plan properties of the selected access plan in the access plan pane in the order the user places them.

The access plan property pane lists all the property names that were specified for the selected Campus plan. This means that the names showing may be different for each Campus Plan.

Adding a Property

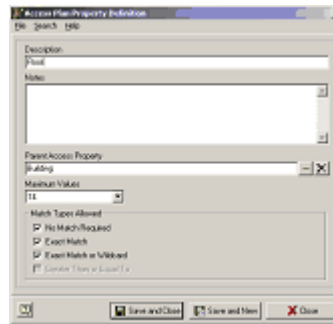
Properties can be defined in a hierarchical way which allows the user to organize multiple buildings, floors and rooms. The move up and move down buttons allow the user to rearrange the properties. This is important when properties have parent properties. Parent properties must be above the child property. If you try to move a child property above its parent, the user will get an informational message saying they cannot do this.

Follow these steps to define a property.

- 1 Select the Plan of which you want to define the property. All the Plans that are defined in the system are displayed in the left hand side of the application.
- 2 Click the Insert (+) button from the Properties section.

Note: The insert, delete, move up, and move down button will be disabled if the access plan selected is read only. Properties that are parents of other properties also cannot be deleted if the child property has one value defined. The user must delete the child property values or the property itself to delete the parent property.

3 Access Plan Definition dialogue opens.



- 4 Enter an easily identifiable description for the property. The Description field allows sixty four (64) characters.
- 5 Enter the notes attached to it. This field is optional and it allows the user to add two hundred and fifty six (256) characters.
- 6 To enable **Parent Access Property** field, you need at least one property defined. If you already have a property defined, click the expand button to select the parent property of the current property. For example, if the current record is a floor, you can select the building as its parent.
- 7 Select the maximum number of properties that can be defined for an access plan. This value also depends on the maximum number of values selected for each Property. Some examples are:
 - a) You can have nine (9) properties if each property sets the maximum values to fourteen (14).
 - b) You can have three (3) properties if you set two (2) properties to fifty thousand, six hundred and twenty four (50624) maximum values and one (1) property to fourteen (14) maximum values.
 - c) You can have five (5) properties if you set two (2) properties to fourteen (14) maximum values, two (2) properties to two hundred and twenty four (224) maximum values, and one (1) property to three thousand and seventy four (3374)
- 8 Once the maximum number of properties has been defined, the insert button will be disabled.
- 9 The next is a group of fields called **Match Types Allowed**. The options available are No Match Required, Exact Match, Exact Match or Wildcard, and Greater than or Equal to. Match values define how exact a Campus Mag has to match to gain access to a Campus Lock. For example, Doors in common areas of a Building most likely do not require exact matches as long as it is made sure that nobody other than the authorized users can access the entrances to the Building. At least one of these options must be checked to save the record. The selection you make here will be selectable when defining Campus Locks in System Manager. Choose the required option from the list by clicking on the check box next to the corresponding option.

Use of Wildcard - Wild Cards allow broadening access rights granted through a Campus lock credential by including all values for one or more properties. Wild Cards are only applicable to properties that allow for wild card matches. With wild card access rights one can have access to all the doors on a specific floor of a building if "Floor" and "Building" are properties of the access plan assigned to the selected door.

 - a) The option Greater Than or Equal To is disabled if either Exact Match or Wildcard or Exact Match is checked.
 - b) Exact Match and Wildcard and Exact Match are both disabled when Greater Than or Equal To is checked.
- 10 Select **Save and Close** to save the record. Select **Save and New** to save the current record and add a new one. Click **Close** to exit the window without saving the record.
- 11 Sorting is not allowed in this grid because the user must place these properties in the order they prefer. Properties that are parents of other properties must be placed higher than their child properties. The grid displays all the data a property has.

Access Property Values

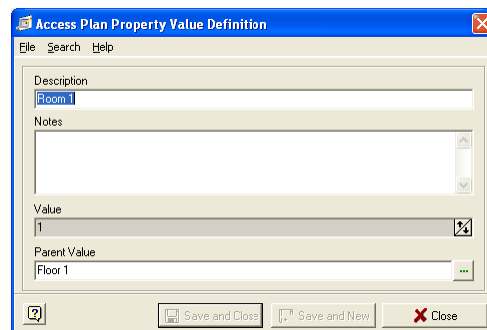
In the lower section of the main window you can define values for each property. Follow these steps:

- 1 Select the Property you want to define the Value for. For example, we can define values for the Property Building.
- 2 Select the **Insert** button (+) from the Access Plan Property Values section. The **Access Plan Property Value Definition** window opens. Enter a description and notes attached to it. If you want to add multiple Values at the same time select, **Options->Mass Add Enabled**. The Description field also informs the user to use the '%' character as the replacement character. There must be at least one '%' character in the description when using the mass add feature.

Example: If the user enters 'Building%' as the description, one (1) as the From, and 5 as the To, the following records will be created:

Building 1
Building 2
Building 3
Building 4
Building 5

- 3 When the dialog is in the **Mass Add Mode**, there are 3 new controls:
 - a) From – The start value for the mass add.
 - b) To – The end value for the mass add.
 - c) Sample – Shows an example of what is going to be created.



- 4 The Value field is always read only because it is automatically generated by the system. In Property Definition if the Match Type, Greater than or Equal to is selected, the system verifies this value while granting access.
- 5 The Parent Value is required if the access property has a parent property. If the property does not have a parent property, this option is disabled and is not required.
- 6 Select **Save and Close** to save the record. Select **Save and New** to save the current record and add a new one. Click **Close** to exit the window without saving the record. A status bar displays when the user starts the save showing the user the progress. Next to the progress bar is a cancel button which allows the user to stop the save in the middle.
- 7 The toolbar has all the standard icons that all other Schlage SMS applications have.

Defining User Types

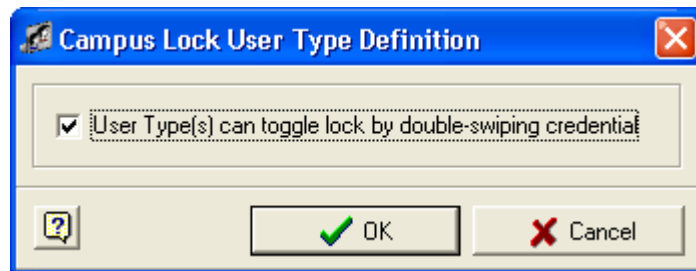
User types define which group of users will have access to the campus locks depending on the timezone and holiday configuration of each lock. There can be between one and sixteen user types with a given name for each.

- 1 Open the **System Manager**. Select **Edit>User Types**. Click on any of the given label.
- 2 The **User Type Definition** window opens. Select the **Enabled** check box to activate the user type. Enter a description and notes attached to it.

The screenshot shows the 'User Type Definition' dialog box. It features a menu bar with 'File' and 'Help'. The main content area includes a 'Description' text box containing the word 'Maintenance', a larger 'Notes' text area, and three checkboxes: 'Enabled' (which is checked), 'Access Blocked', and 'Revalidation Allowed at Kiosk'. Below the checkboxes is a label 'Days Credential Will Expire After Revalidation (zero indicates valid for today only)' followed by a numeric input field showing '0' and a spinner icon. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

- 3 **Access Blocked** allows the user to block or unblock access to a whole group. If this changes, every lock must be reprogrammed for this function to take effect.
- 4 Click **OK** to save the record. **Cancel** closes the window without saving the record.

User type must be specified when a campus lock credential is created or modified. While defining Campus Locks, you can grant access to different user types. It also gives an option to the selected user type(s) to toggle the door by double swiping credential.

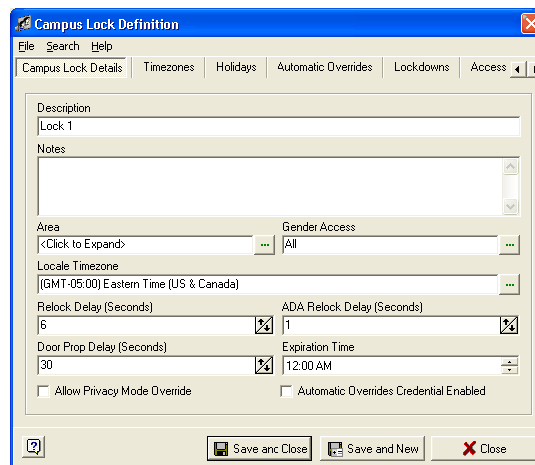


While defining campus credentials for cardholders, the enabled user types are available for assignment.

Defining Campus Locks

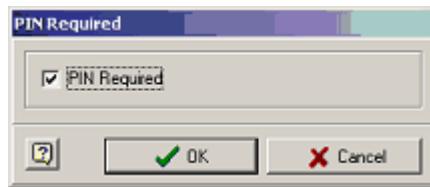
Follow these steps to define a new campus lock.

- 1 Open the **System Manager** application. Select **Hardware Definitions**. Select **Campus Locks**.
- 2 Select the Insert button from the grid section. The **Campus Lock Definition** window opens. The dialogue opens the **Campus Lock Details** section. Details shows the functions and controls for the basic access right assignment for a Campus lock.



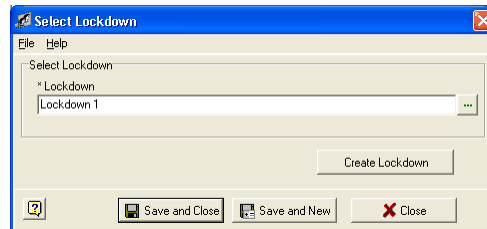
- a) Enter a description and notes.
- b) **Area** is a required field. It is used for lock organization and security. It has nothing to do with access control for the lock.
- c) The next setting is **Gender Access**. Campus Locks can be set to allow only access with credentials that have the gender of the user set. Click on the expand button to see a list with available options. The options are "All", "Male", "Female" and "other", with "All" being the default. This setting is typically used to limit access to bathrooms or locker rooms
- d) **Locale Timezone** is required and is the timezone the lock is in.
- e) **Auto Relock Delay** is a required field and must be between one and two hundred and fifty four (254) seconds. This is the amount of time the lock will stay unlocked after a valid access.

- f) **ADA Relock Delay** can be assigned to each Campus Lock. The ADA Relock Delay of a Campus Lock overrides the standard Auto Relock Delay time configured for a Lock if the value for the ADA Relock Delay is greater than the standard Relock Delay. It further enables the ADA Relock Delay function of a Campus Lock.
 - g) **Door Prop Delay** - Enter the duration you want the door to be open in seconds. If the door is open for more than the time specified in this field, the system created an audit to indicate that the door is held open.
 - h) **Expiration Time** sets the time access cards expire on their Expiration Date for this campus lock. This setting is individual to each Campus Lock and should be set based on the local policies or needs. The default is 12:00 AM. Click on the hour, minute, or AM / PM position and type in the desired values in the specific position or use the up and down cursor keys on the keyboard.
 - i) **Allow Privacy Mode Override** is a required field. If this field is enabled, it allows cards to override a lock that has been placed in privacy mode. If this field is unchecked only cards specifically assigned to this particular door will have access.
- 3 Next step is assigning time zones. Select the **Timezone** tab. Click the Insert (+) button. Select the appropriate timezone, and click **OK**. Double click on the selected time zone to enable the PIN Required option. You can attach a timezone with two intervals with Campus Locks only if the interval of that timezone is a spanning midnight timezone. The first interval should end at 11.59.59 PM and the second interval should start at 12.00.00 AM. The intervals must align at midnight on successive days.



- 4 If this option is selected, and while assigning credentials the option PIN Requirement option is set as "As Defined by Timezone", the cardholder will have to always use a PIN number along with the credential to gain access to this particular lock.
- 5 Next click on the **Holidays** tab to select the holidays for the lock. Select the + sign to add holidays. All the holidays defined in the system are displayed. The plus icon lets the user select a single holiday and the function for the holiday. The binoculars (search) allow the user to select multiple holidays and then select one function which all the holidays will receive. Click **OK**.
- 6 Select an offline function to apply to the lock.
- **Passage** - The offline device will allow access during the specified holiday.
 - **Secured** - The offline device will be locked and will not allow access through the door during the specified holiday.
 - **Secured Lock Out** - The offline device will not allow access, but will allow people with special credential to go through the door during the specified holiday.
- 7 Select **Save and Close** to save the information and close the dialog. Select **Save and New** to save the current information and enter new information. Select **Close** to close the dialog.

- 8 Click on the expand button near the **Lockdown** field to select a pre-defined lockdown. The **Create Lockdown** button allows you to define a new lockdown. Note that you cannot attach lockdowns with the same time schedule to an offline lock. See the Lockdown Definition section in System Manager for further details.



- 9 Next select an **Access Plan** for the lock. You need to select the Campus Plan, various Properties and appropriate Values for Campus Lock based on the records defined using the Access Plan Definition. The **Campus Lock Definition** cannot be set before at least one Access Plan is completed. The window shows the Access Plans, Properties and the Property Values. The amount of controls and options that appear in Access plan section depends heavily on the Access Plan Definition, and here especially on the Access Plans..
- 10 Property values for Access Plans can be added or deleted from this window. They will immediately also be seen in Access Plan Definition program.
- 11 You need to have at least Read/Write permissions to **Access Plan Definitions** program to create property values from this window. See the section **Defining Access Plans** for Campus Locks for further information.
- 12 Now select the user types that will have access to this lock. All the user types enabled and labeled are available for selection. Up to 16 user types can be added to a lock. Each user type can have up to 16 timezone added to them. Only timezones added to the campus lock itself will be selectable. If a timezone is deleted from the lock, it will also be deleted from all the user types using it. At least one user type and one timezone must be selected to save a lock.
- 13 Select **Save and Close** to save the record. Select **Save and New** to save the current record and add a new one. Click **Close** to exit the window without saving the record.

Programming Automatic Overrides for Campus Locks

Automatic Overrides can be programmed for campus locks using the ARO program. Please refer to the chapter on **Automatic Overrides>Auto-unlock Offline Locks** to know more about this feature.

Assigning Access Rights to a Campus Lock

Refer to Cardholder Definitions chapter for detailed information on assigning access rights to Campus Lock.

CCTV

CHAPTER 42

Introduction

The purpose of the **Schlage SMS CCTV Universal Interface** is to give the ability to activate any RS232 device such as a switcher to provide video capturing at the point of alarm activation. While this software can be used for CCTV Video interface it can also be used with various other equipment from fire sprinkler systems to automatic security lighting.

In the System Security module, add **Camera.exe** to the System Launcher and assign the appropriate security rights. (Refer to the System Security chapter for details on how to do this.) Name it "CCTV Camera Control".

Accessing the application

- 1 Open the **System Launcher** by double clicking the Launcher icon on your desktop or select **Start>Programs>Schlage SMS>Schlage SMS**.
- 2 The login window, opens. Enter your user id and password.
- 3 In the System Launcher window, double click on CCTV Camera Control icon.

Overview

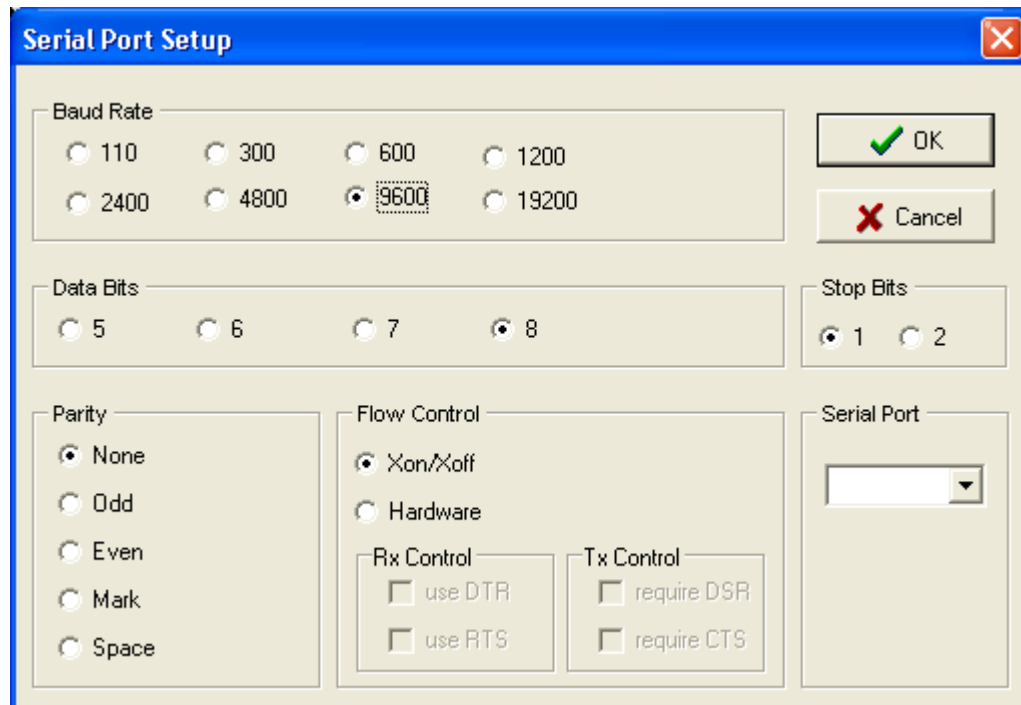
The main window of CCTV Camera Control launches when the module is opened. Options are accessed from both the Menu Bar and the Toolbar. Camera events are programmed and displayed in the Trigger Event section and the **Communication Status** display window shows information that is being received from the multiplexer device.

Programming

- 1 In the **CCTV Camera Control** window, select **Tools>Serial Port Initialization** option. The sub window **Serial Port Setup** becomes active.

Note: This screen will be the active window when CCTV is opened for the first time after installation of the **Schlage SMS**. For the proper settings of the device that will be attached, please refer to its manual.

- The manual settings should match those of the **RS-232C** port. Click **OK** to accept the settings and return to the main window.



- Click the **New** icon to open a new **Camera Trigger Editor** window. Select a device from the **Device Selection** tree.
- Select a Time zone** to determine when the action is active. Select a **Transaction** to determine what triggers the action. This is found in the **Filters Frame**.
- In the **Output String** Frame, click on the expand button in the **Command** String field. This will open a **Control Characters** Window. The control characters you select will be based on the type of device you have and valid command strings for that particular device.

Note: These valid command strings can be found in the manual packaged with the device.

- Once you have selected your **Output String Command** click **Save**. You can forward the commands to the attached device using the Send button. Transmissions to and from the attached device will be displayed on the main screen under the **Communication Status** section.

Serial Port Communication Test

- For testing, connect a jumper from Pins 2 & 3 on the port. This will take "Transmit Out" and jumper it to "Receive In". When sending the command out (To Switch) you should see (From Switch) your string command.

Menu Options

File Menu

- 1 **Verbose** – This is a toggle option that allows more detailed messages to display in the Communication Status window when checked. The default is unchecked.
- 2 **Exit** -This option closes the CCTV Camera Control Module.

Edit Menu

- 1 **New** – Creates a new Trigger Event. When this option is chosen, the Camera Trigger Editor sub window is opened. Enter a Device, Timezone, Transaction and Output String. To send the command to the camera, select the Send button. To save the trigger and program a different event, select the New button. To save and close the sub window, select the Save button. The trigger will display in the main window under the Trigger Events section.
- 2 **Modify** – Allows Editing of a currently highlighted Trigger Event.
- 3 **Delete** – Deletes the currently highlighted Trigger Event.
- 4 **Modify** – Allows Editing of a currently highlighted Trigger Event.
- 5 **Delete** – Deletes the currently highlighted Trigger Event.

Tools Menu

- 1 **Status Bar** - Toggles the Status Bar on and off. The Status Bar is located on the bottom right of the Communication Status window. It will display Comport, SP, Time and Date information.
- 2 **Tool Bar** - Toggles the Tool Bar on and off. When unchecked, the toolbar will be hidden.
- 3 **Serial Port Initialization** - Opens the Serial Port Setup window to allow configuration of the serial port for communications with the attached device.
- 4 **Send Command** - Will send the currently highlighted Trigger Event to the attached device.
- 5 **Clear Status Display** - Clears all messages from the Communication Status window.
- 6 **Append Carriage Return** – Puts a carriage return character at the end of every command. This is required for some devices.

Toolbar Icons

- 1 **New** - Creates a new Trigger Event.
- 2 **Edit** - Allows editing of the currently highlighted Trigger Event.
- 3 **Delete** - Deletes the currently highlighted Trigger Event.
- 4 **Send Command** - Sends the currently highlighted Trigger Event to the attached device.
- 5 **Clear Status Display** – Clears the Communication Status window.
- 6 **Exit** - This will close the CCTV Camera Control Module.

SVTR

CHAPTER 43

Introduction

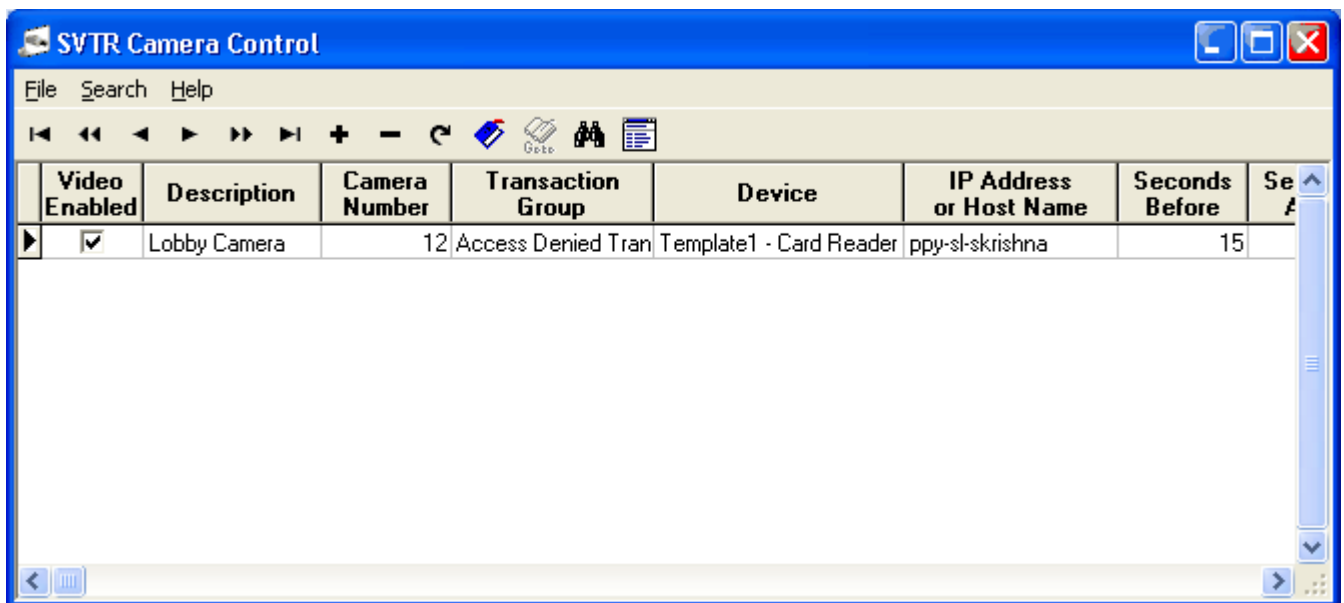
The **Schlage Video Transaction Retrieval System** (SVTR) is a computer based video surveillance recording and retrieval system that automatically captures and compresses high resolution digital video images of various types of transactions. It is the video interface to the **Schlage SMS**. It allows a user to view the video associated with a transaction from a Schlage client workstation. The system records an event with a pre-event of 15 seconds and a post-event of thirty (30) seconds.

Accessing the application

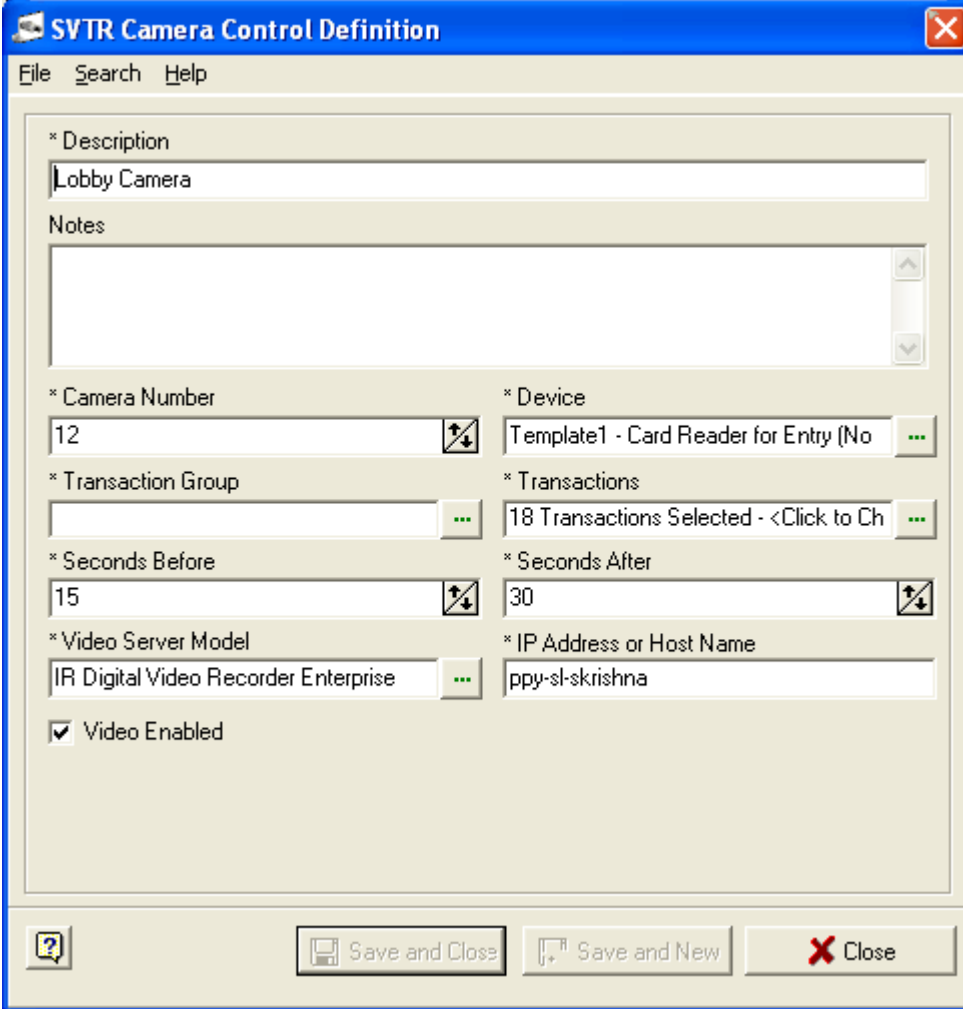
The SVTRPlay5 can be launched from five (5) different programs in the **Schlage SMS** Launcher: They are "Transaction Monitor", "Previous Transaction", "Alarm Monitor", "Previous Alarm" and "Alarm Graphics".

Working with SVTR Camera Control

- 1 Click on **SVTR Camera Control** in the **Schlage SMS** System launcher.



- 2 To add a definition click on the + sign.
- 3 The following window is displayed.



The image shows a software window titled "SVTR Camera Control Definition". It has a menu bar with "File", "Search", and "Help". The main area contains several fields and controls:

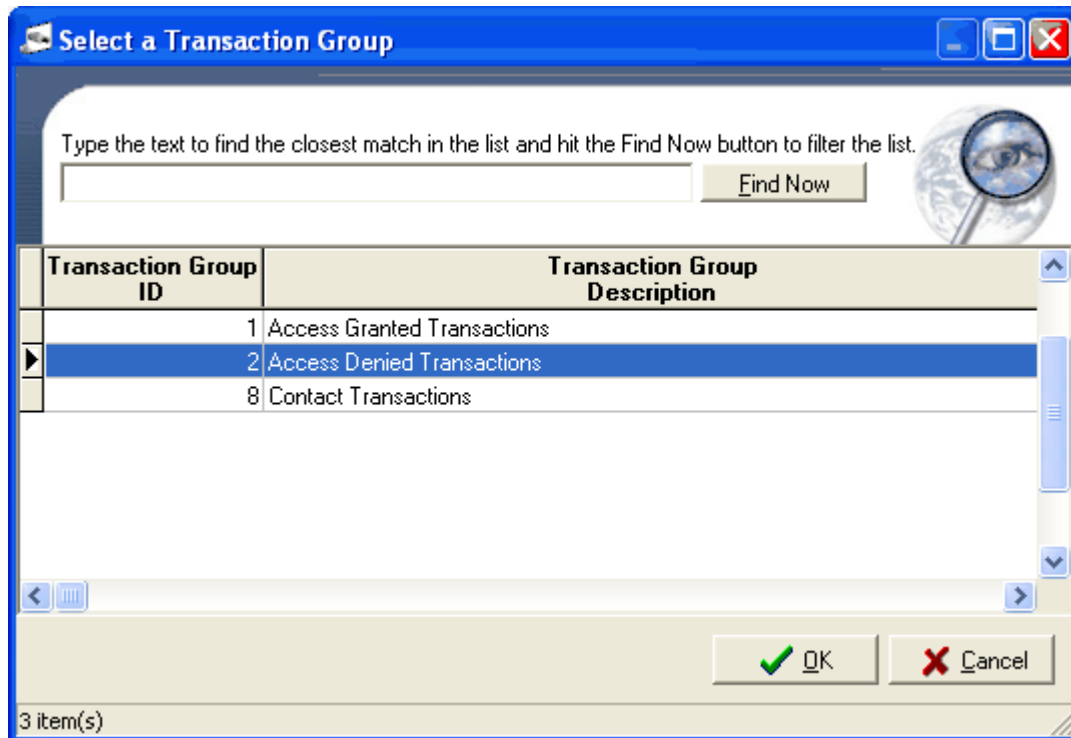
- * Description:** A text box containing "Lobby Camera".
- Notes:** A large, empty text area with a vertical scrollbar.
- * Camera Number:** A text box containing "12" with a small icon to its right.
- * Device:** A dropdown menu showing "Template1 - Card Reader for Entry (No" with a small icon to its right.
- * Transaction Group:** A text box with a small icon to its right.
- * Transactions:** A dropdown menu showing "18 Transactions Selected - <Click to Ch" with a small icon to its right.
- * Seconds Before:** A text box containing "15" with a small icon to its right.
- * Seconds After:** A text box containing "30" with a small icon to its right.
- * Video Server Model:** A dropdown menu showing "IR Digital Video Recorder Enterprise" with a small icon to its right.
- * IP Address or Host Name:** A text box containing "ppy-sl-skishna".
- Video Enabled:** A checkbox that is checked.

At the bottom of the window, there are three buttons: "Save and Close", "Save and New", and "Close".

Configuring Transactions, Devices, Alarms etc.

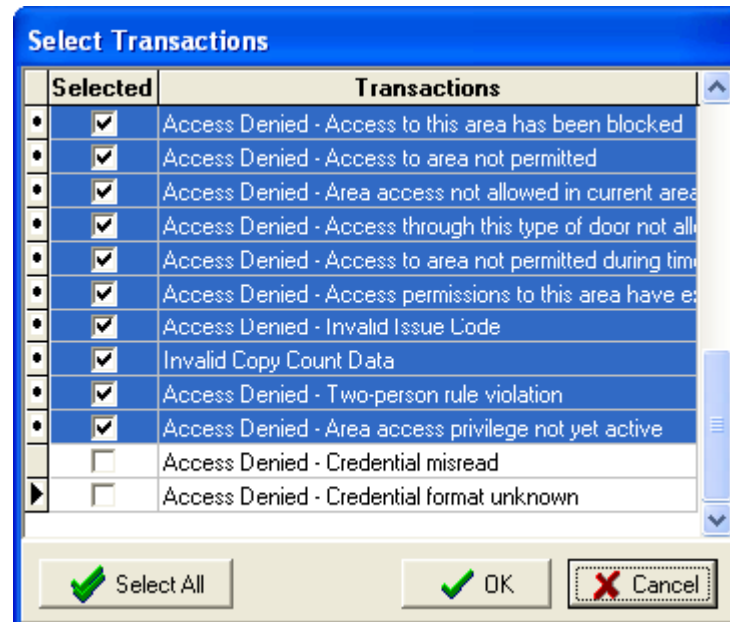
- 1 Enter a description for the camera in the Description field. A maximum of 64 characters are allowed.
- 2 Next enter any related notes in the Notes field.
- 3 Select the Number of the camera that is to be associated with the transaction.
- 4 Select the device that the camera will be used for monitoring.
- 5 Select the type of transaction group you want the video to be displayed on and click OK.

E.g. Access Granted, Access Denied or Contact Transactions.

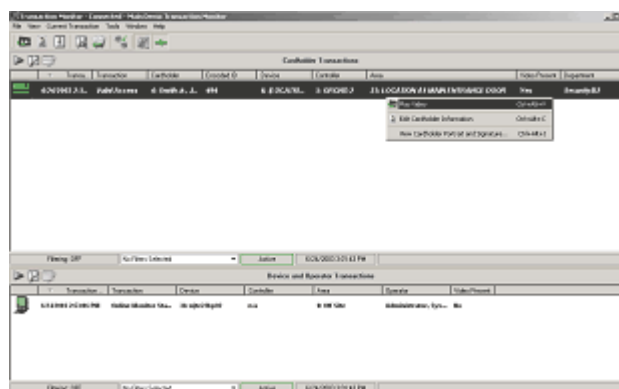


- 6 Select the transactions you wish to view the video for and click **OK**.

E.g. Access Valid, Contact Active.



- 7 Select the device from which the video is triggered. and click **OK**.
- 8 Specify the server name (host name) of the video server where the camera is located is typed in this box.
- 9 Check off the box **Video Enabled**. This will enable the stored video for this definition.
- 10 Click **OK** to complete the camera definition.
- 11 When a transaction occurs, if it has been defined in the SVTR camera definition, when you highlight the transaction in the Transaction Monitor and right click, you will see a **Play Video** box.



IR Viewer

CHAPTER 44

Introduction

The **IR Viewer** is the video interface to the **Schlage SMS**. It allows the user to view the video associated with a transaction from a Schlage client workstation. The system records an event with a pre-event of 15 seconds and a post-event of 30 seconds.

This application consists of two components:

1 Playback Viewer Component

Capture and Playback video based on a set of parameters.

Parameters allow the selection of the DVR, Date, Beginning & Ending Times, Instance Time, and Camera

Save the video in one of two formats:

MJPEG: Proprietary format for **Schlage SMS**

AVI: Audio Video-Interleave (Windows' format)

2 Live Viewer Component

Play video in Live Mode is based on a set of parameters. Parameters allow the selection of the DVR, Date, and Camera. The Live Window has no buttons.

System requirements for IR Viewer

The following Operating Systems are supported:

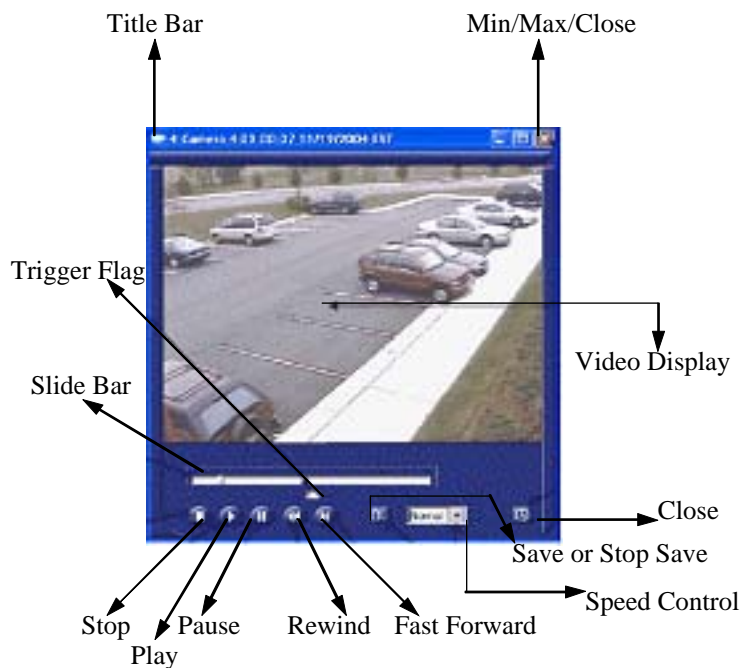
1 Microsoft® Windows™ XP

- Version 2002
- Service Pack 1 and Service Pack2

2 Microsoft® Windows™ 2000

- Built on NT Technology
- Version 5
- Service Pack 4

Working with IR Viewer



Playback Viewer screen explanation

Playback Viewer is used to view recorded video or capture a particular video segment to a file (AVI or MJPEG).

The following is the explanation of each buttons seen on the screen.

- 1 **Title Bar** - Identifies the camera number, camera title, video tracking time, date, time zone.
- 2 **Slide Bar** - Provides the capability to follow the movie progress, or capture the thumb and move it to a new position.

Note: Dependent upon the frames captured within the time frame specified, the slide bar may not seem to start at the very beginning or end at the very end.

- 3 **Trigger Flag** - This instance marker will indicate the location of the `-i` parameter during the video progression.
- 4 **Stop Button** - Halts the video. Pressing Stop and then Play will result in the video starting from the beginning.
- 5 **Play Button** - Moves the video forward based on the recorded speed from the beginning.

Note: With the majority of Operating Systems, the video will automatically open in play mode – others will require that the Play Button be pressed.

- 6 **Pause Button** - Interrupts the progression of the video. Pressing the Pause and then the Play button will result in the video resuming from the point of interruption.
- 7 **Rewind Button** - Moves the video backwards at 8x the speed. Once the video has reached the beginning time and the Rewind Button is pressed a second time (while it is still red) the video will begin to display the video prior to the begin time specified. Note: It may be necessary to press the Rewind Button twice in order to get it to move past the start time.
- 8 **Fast Forward Button** - Moves the video forwards at 8x the speed. Once the video has reached the end, pressing the Rewind Button again (while it is red) will result in the video continuing past the requested clip.
- 9 **Speed Control** - Allows the user to control the speed of the Fast Forward and Rewind functions.
- 10 **Save Button** - Allows the video to be saved to a file (AVI or MJPEG formats). This button is also used to stop the save, prior to completion.
- 11 **Close Button** - Shuts down the application and closes the screen.
- 12 **Video Display Area** - This part of the screen allows viewing of the video.
- 13 **Min/Max/Close Icons** - Provides ability to minimize to the desktop taskbar, maximized to $\frac{3}{4}$ full screen, or close the application.

Note: When the Playback Viewer is initially launched, all buttons will be inactive. The buttons will change from blue to red as they are activated. If the focus is moved off of the IR Viewer application, the buttons will revert back to blue until the focus is returned.

Button combination functions

- 1 **Stop/Play** - Video is halted and then starts from the beginning.
- 2 **Pause/Play** - Video is halted and then resumes from the point of interruption.
- 3 **Fast Forward/Play** - Video is played forward at the speed selected and then is played from the beginning at normal recorded speed. Play once video has completed: Video is reset to the beginning.
- 4 **Fast Forward/Stop/Play** - Video is moved forward at the selected speed and is then halted and then resumes from the very beginning.
- 5 **Rewind/Stop/Play** - Video is moved backward at the selected speed and is then stopped and then resumes from the very beginning.
- 6 **Fast Forward while video is at the end/Pause/Play** - Video continues to progress PAST the end time; video is then halted; video continues in play mode from the point of interruption. In this scenario the video will be in play mode outside the set end time.
- 7 **Rewind while video is at the very beginning/Pause/Play** - Video is progressing prior to the start time at the selected speed; video is then halted at the point of interruption; once play is pressed the video will continue in play mode outside the set start time.

Saving a video clip to a file

The Playback Viewer allows a video segment to be saved to a file in either an AVI or MJPEG format.

- 1 MJPEG (proprietary format of Schlage) - These files can only be viewed via the VCR Application.
- 2 AVI formats can be viewed via Media Player, QuickTimePlayer, etc.
- 3 To begin the process (i.e. open file), click on the Save button.

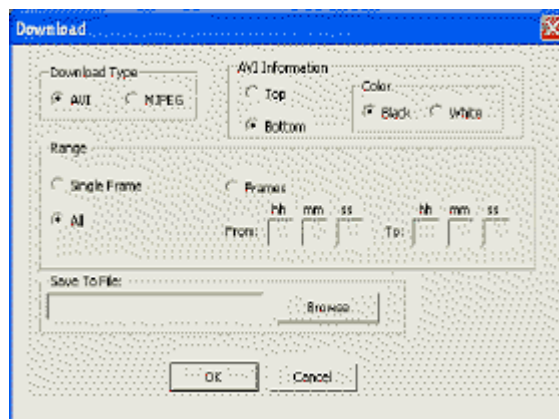
- 4 To end the process, prior to completion press on the Save button a second time.
- 5 Multiple files can be saved during the same Viewer session as long as each is started with the Save button and ended with the Stop button.
- 6 Save.

Save an AVI file

- 1 Click on the **Save** button on the **Playback Viewer** screen to create an AVI video file.

Saving an AVI file as a dialogue

- 1 Click on the Browse Button to select the file location and enter the file name. (Note: The file name will automatically be populated with the word 'video.' In order to create a different name for this file, type in a new name.
- 2 In the AVI Information Section, click on the location and text color for the video clip title information.
- 3 Select a Range: Single Frame – just the frame being viewed; Frames – enter the beginning and ending times of the video segment (note: this time frame does not have to be within the segment being viewed); All – the entire video segment currently being viewed in the Player Window will be saved.
- 4 Press the OK button to select a compression method (see next slide).



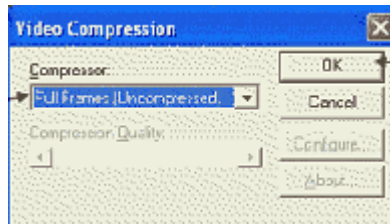
Video Compression dialog

The Video Compression dialog box will only appear for AVI files.

Purpose - Compression technology makes the files smaller so they do not use as much space on your PC. Typically, the more compression you use, the smaller the file is; however, the picture quality of a highly compressed file may not be as clear. The trade-off is that when files are smaller, you can store more content on your hard drive.

- 1 Select one of the following options for the AVI file:
 - Full Frames (Uncompressed)
 - Intel Indeo ® Video 5.11
 - Microsoft Video 1
 - Cinepak Codec by Radius

Note: The options displayed in the Compressor list will be dependent upon the options installed on the PC. These are not part of the IR Viewer installation package. Not all compression methods are certified for use with the Viewer application. The options listed above have been confirmed to work with the IR Viewer Application. Both Full Frames and Intel Indeo ® Video Version 5.11 have been identified as providing the best results with this application.

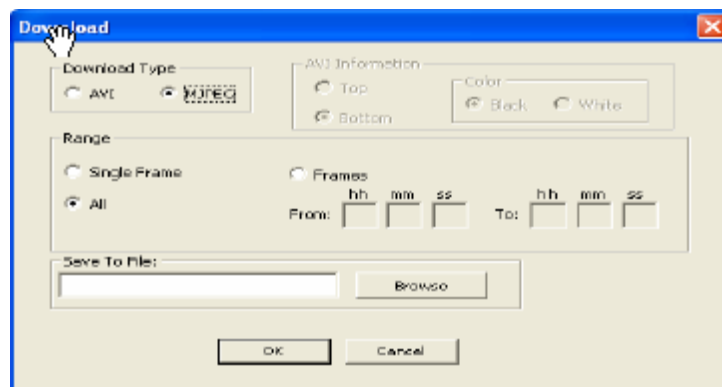


Saving a MJPEG file

- 1 Click on the **Save** button on the **Playback Viewer** window to create a MJPEG video file.

Saving MJPEG file as a dialog

- 1 Click on the **Browse** Button to select the file location and enter the file name. (Note: The file name will automatically be populated with the word 'video.' In order to create a different name for this file, type in a new name.
- 2 Select a Range: Single Frame – just the frame being viewed; Frames – enter the beginning and ending times of the video segment (note: this time frame does not have to be within the segment being viewed); All – the entire video segment currently being viewed in the Player Window will be saved.
- 3 Click **OK** to select a compression method (see next slide).



- 4 To end the save process, at any time, click **Save** on the **Playback Viewer** screen.
- 5 To monitor the status of the save, hold the cursor over the **Save** button.
- 6 When the save is in progress the context help will display "STOP SAVE" and when the save is complete the help will display "SAVE AS FILE."

- 7 To review the saved MJPEG video clip, open IR's VCR Application.



STOP SAVE
or
SAVE AS FILE

Guest Pass Settings

CHAPTER 45

Introduction

Before you begin using your Guest Pass System, you may need to configure the settings appropriately. The Guest Pass Settings customizes the Guest Pass System. It is the settings that determine what information is required and they control the screens that an operator sees within the **Guest Pass System** module. Users have the ability to view and track Pending, Signed In and Signed Out guests in multiple Locations (See Glossary of terms for details). Requirements and instructions for the Guest Pass System can be configured using the different tabs found in the Guest Pass Settings module. The Guest Pass System module does not allow adding a guest into the system until all required information is given.

The **Guest Pass Settings** is a global application and the changes made in the settings immediately take effect.

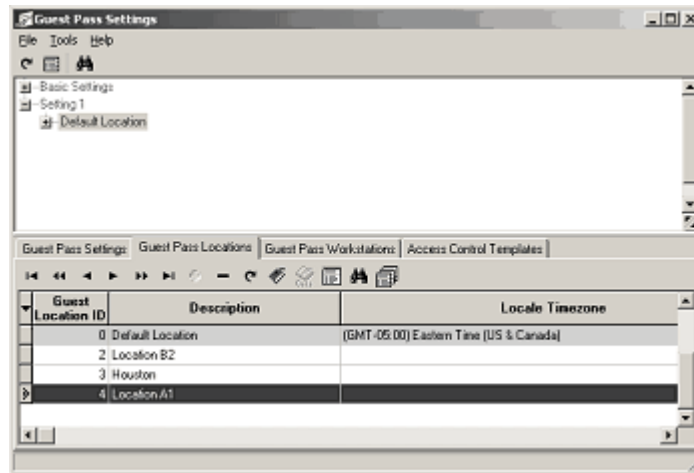
The system allows the user to create an infinite amount of settings, and attach to different locations. All the fields pertaining to each setting are displayed in the main window of the Guest Pass System.

Accessing the application

- 1 Open the System Launcher by double clicking on your desktop icon called **Schlage SMS**.
- 2 Double click on the Guest Settings icon. The program window is displayed.

Define Settings

- 1 To select and expand a setting, click on the **Guest Pass Settings** tab on the program window.



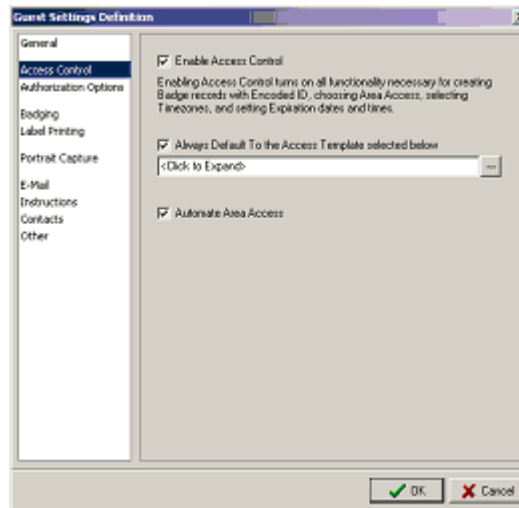
- 2 Click on the + icon to open the **Guest Settings Definition** window.
- 3 Click on the options available on the left hand side of the window to define each setting.

General Setting

- 1 Click on the option **General** located on the left hand side of the window. Enter a description for the setting in the **Description** field and the notes attached to it in the **Notes** field. Click **OK**.

Access Control

Note: This setting should be activated to assign access privileges while adding a guest.



- 1 **Enable Access Control Requirement** - Select this option to make the related features (shown on this window) available. This option must be enabled in order to provide access to Areas and assign badges to guests (see glossary of terms for details). If you do not enable this option, while adding a guest all the steps related to access control are skipped. The following are the related steps.
 - a) Enter the Encoded ID of the Badge Assigned to the Guest.
 - b) Please Select the Guest's Access Time.
 - c) Select the Area Sets for this Guest.
 - d) Select the Time zone for this Guest.
- 2 **Always Default to Access Template** - Select this option to designate a default Area Access Template to be used while adding guests. Once configured, the Guest Pass System defaults to the Area Sets and Time zones included in the selected Template. Users may change these options while adding a guest, if necessary.
- 3 **Automate Area Access** - Select this option to automate the steps required to give Area Access. The following steps are not offered to the user while adding a guest and the system applies the settings defined in the default template.
 - a) Access Time
 - b) Area Sets

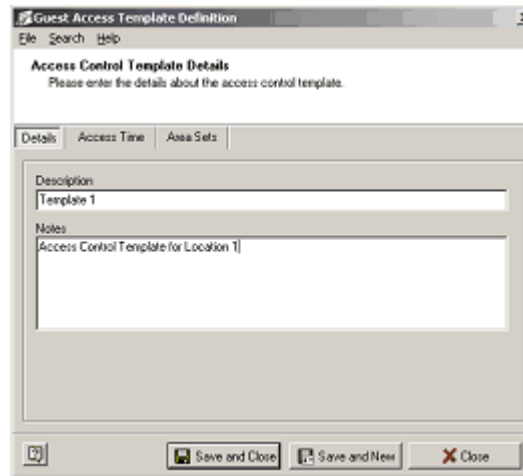
Note: The operator can override the Area Access automation feature by holding down the Ctrl key prior to advancing to this page in the Wizard.

Defining a Template

The Access Control Template allows the user to define and apply the components of area access (Area Sets and expiration time) easily. The Guest Pass System uses the Area Sets and the expiration time defined in the template while signing in a guest. Follow these steps to define an access control template.

- 1 On the **Guest Pass Settings** window, click on the tab called Access Control Template.

- 2 Click on the + sign to open the **Guest Access Template Definition** window.



- 3 The window defaults to the **Details** tab. Enter the description for the template in the **Description** field. Add the notes pertaining to the template in the **Notes** field.
- 4 Next, click on the **Access Time** tab. Here define the expiration time for the guest's Area access. The user can specify the number of hours After Sign In time that the guest will have access to an area or, select the time of the Sign In day that access will expire.
- 5 Next, click on the **Area Sets** tab to select the Area Sets the guest will have access to. Click on **Add** to add Area Sets to the list. You can add as many Area Sets as you want. To remove an Area Set from the list, highlight the Area Set and click **Remove**. If you want to clear the entire list click **Clear List**.
- 6 Guest access templates now handle area set permissions as follows:
 - a) The user will not be able to manually select an access template unless they have at least read-only permissions to all the area sets in the template.
 - b) If the settings for the workstation is set to automatically default to a specific access template that does not pass rule #1, the user will be forced to select a new template or to enter the access information manually.
 - c) If the settings for the workstation is set to automate area access completely using a specific template that does not pass rule #1, the user will be forced to select a new template or to enter the access information manually.

Authorization options

The term authorization refers to security privileges, usually given only to a few operators, which allows them to Authorize guests for Sign In. Read/Write privileges to the Guest Pass System module must be granted to the operator. Guests must be Authorized prior to Sign In.

1 Authorization Question

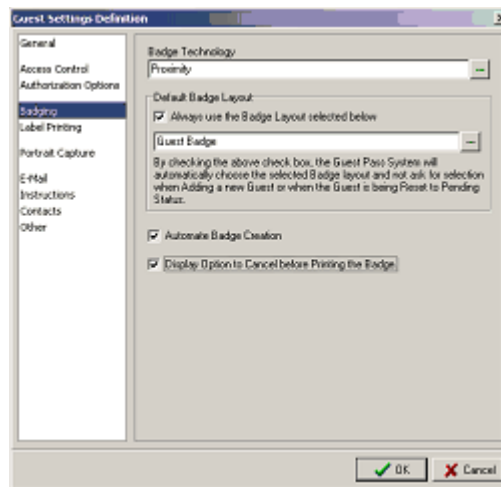
Always Authorize when Allowed - If this option is enabled, when an operator adds a new guest to the system, the guest will be automatically authorized. The system skips the step that prompts the operator to choose between authorize or not to authorize. The guest is automatically authorized, only if the operator has authorization privileges.

2 Sign In Question

Always Sign In when Allowed - Selecting this option will cause the guest to be automatically Authorized and Signed In when added to the system, without prompting the operator. The appropriate privileges must be granted to the operator.

Badging

The Guest Pass System allows the user to issue badges with Encoded ID to the expected guests. Badges are assigned to the guest who has access control privileges during their visit. The different options on this window allow the user to specify the badge technology and the badge layout they are going to use while creating badges. The following are the descriptions for each option.



Note: Badge printing must be enabled in the Workstation Definition in order to be performed by the operator. You have to select the Enable Access Control option to activate and configure the Badge Printing features.

- 1 **Badge Technology** - Click on the expand button to specify the appropriate badge technology you want to use for creating badges. The Guest Pass System will automatically choose this badge technology while creating badges.
- 2 **Default Badge Layout**

Always Use the Badge Layout Selected Below - Enabling this option forces the operator to use the selected badge layout while creating badges. The steps to select a badge layout while adding a guest in the Guest Pass System will be skipped. Click on the expand button to select a badge layout.
- 3 **Automate Badge Creation** - Enable this feature to make all the available features corresponding to badge creation automatic. The system automatically chooses the next available encoded id, default badge layout and badge technology that are set here. If this option is selected the system skips the following steps while signing in a guest.
 - a) Select a badge layout
 - b) Select encoded id

Note: The operator can override the badge automaton feature by holding down the Ctrl key by holding down the Ctrl key prior to advancing to this page in the wizard.

- 4 **Display Option to Cancel Before Printing the Badge** - Enabling this feature will display a message which provides the user with the option to cancel or proceed with badge printing in the final step of Sign In. Badges will be printed by default when disabled.
- 5 Click **OK** to save the setting and exit to proceed with **Encoded ID Settings**.

Encoded ID Settings

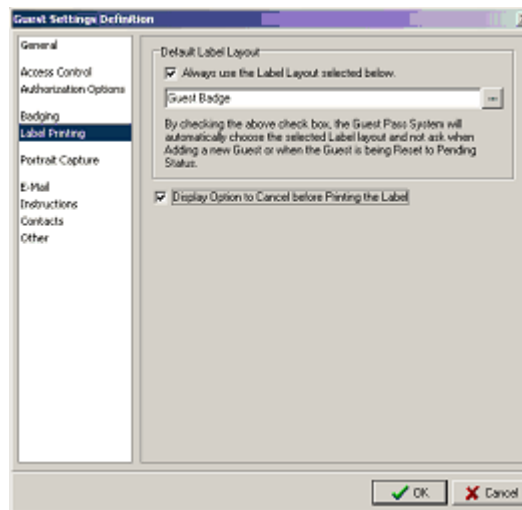
The Guest Pass System provides a feature called **Get Next Available**, which allows you to generate Encoded ID automatically. In the Guest Pass Settings you can set a starting and maximum value. When you create a badge, the system will assign only an unused and unique ID within your range. There is also an option to reset the Encoded ID range manually.

- 1 Click on **Tools>Global Settings**. In the Guest Pass Global Settings window fill in the following information.
 - a) **Starting Encoded ID** - You can set a value here which will be used as the first Encoded ID of your new badge by the Guest Pass System. If the starting value is already being used, the system will choose the next available value for the ID.
 - b) **Maximum Value** - Here you can specify the maximum value for the Encoded ID.

Label Printing

The Guest Pass System allows the user to issue labels to expected guests. Label printing is enabled via the Workstation definition window. The options on this page customize the label printing features.

Here the user can specify the default label layout and display the option to **Print** or **Cancel** label printing at Sign In. The following are the options related to this feature.



- 1 **Default Label layout** - Always Use the Label Layout Selected Below - Enabling this option forces the operator to use the selected label layout while creating badges, skipping the steps for selection in the Add Guest Wizard. Click on the expand button to select a badge layout.
- 2 **Display Option to Cancel before Printing the Label** - As in Badge printing, enabling this feature will display a message which provides the user with the option to cancel or proceed with Label printing in the final step of Sign In. Labels will be printed by default when disabled.

Image Verification

The Guest Pass System allows the operator to capture an image of the guest while adding or signing him/her into the system. Enabling the options available on this window forces the operator to verify it during signing in and signing out.

Note: To capture images you need to enable and specify the Portrait Capture Device in the Guest Pass Workstation Definition.

- 1 **Require Image Verification On Sign In** - This option forces the operator to verify the identity of the guest. When the operator signs in a guest, the system displays a previously captured image for verification.
- 2 **Require Image Verification on Sign Out** - This option performs the same function as the Sign In option, during the Sign Out process.

E-Mail

The features in this section configure the Guest Pass System to send e-mail messages, with or without the portrait, to the person the guest is visiting while signing in and/or signing out guests.

Note: The operator must have access to an SMTP E-MAIL SERVER to use this feature.

- 1 **Enable E-Mail** - Select this option to activate and configure e-mail settings. When the operator adds a guest, the system prompts the operator to enter the e-mail address of a person who should be notified when the guest is signed in and/or out.

The screenshot shows the 'Guest Settings Definition' window with the 'E-Mail' tab selected. The left sidebar lists various settings categories: General, Access Control, Authorization Options, Badging, Label Printing, Portrait Capture, E-Mail (selected), Instructions, Contacts, and Other. The main area contains the following settings:

- ☒ **Enable E-Mail**
- E-Mail Enabled Features:**
 - ☒ Send E-Mail when Guest is Signed In
 - ☒ Send E-Mail when Guest is Signed Out
 - ☒ Send Portrait with E-Mail if one Exists
- E-Mail Server Settings:**
 - SMTP Server URL or Address: [Your E-mail Server Name]
 - From E-Mail Address (i.e. geoffrey@anywhere.com): [Your email address]
 - From Name (i.e. Jane Doe): [Your name]
 - Reply To E-Mail Address (i.e. replyto@anywhere.com): [Your email address]
 - User Login Name (If server requires authentication): [Operator's login id]
 - Password (If server requires authentication): [password]
 - SMTP Port Number (25 is default): [25]

At the bottom right are 'OK' and 'Cancel' buttons.

E-Mail Enabled Features

The following are the options related to this feature.

- 1 **Send E-Mail when the Guest is Signed In** - Enabling this option allows the operator to announce a guest's arrival to people in a "guest signed in e-mail list".

- 2 **Send E-Mail when the Guest is Signed Out** - This option works the same as the Sign In option, during Sign Out.
- 3 **Send Portrait with E-mail if one exists** - If this option is selected, a portrait of the guest will be included with the activated e-mails.

E-Mail Server Settings

- 1 **SMTP Server URL or Address** - The IP address or URL of the SMTP server should be specified. This host name can be any valid SMTP server with the capability of supporting standard SMTP mail format.
- 2 **From Name** - Enter the name of the person or company who is sending the e-mail.
- 3 **From Address** - Specify the e-mail address from which the e-mail is sent.
- 4 **Reply to Address** - Specify the e-mail address to which you want to receive responses.
- 5 **User Login Name** - Your login name to the SMTP Server should be specified here.
- 6 **Password** - User's password to the SMTP Server.

Note: Login name and password are required only if the outgoing e-mail requires authentication.

- 7 **SMTP Port Number** - Default is 25.

Instructions

The Guest Pass System provides an easy way to add instructions to follow during signing in a guest and upon signing out. Using this feature the operator who is creating a pending guest record (the guest not signed in) can provide required instructions that are displayed later. You can specify when these messages should be displayed (upon signing in or signing out). The following are the options that you can use to enable these features.

- 1 **Enable Instructions** - Select this feature to make the other options on this window available. The operator will be able to enter instructions when adding Pending guests, which may be displayed during **Sign In** or **Out**.
- 2 **Automatically Pop-up Instructions on Sign In** - If this option is selected the instructions are displayed when the guest is signed in.
- 3 **Automatically Pop-up Instructions on Sign Out** - If this option is selected the instructions are displayed when the guest is signed out.

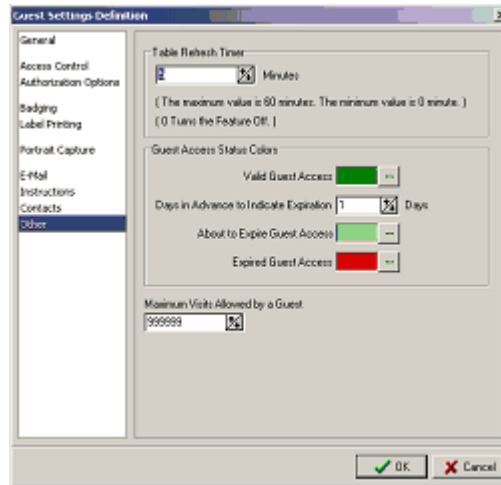
Contacts

When the operator creates a guest record, the Guest Pass System gives an option to add names of primary and secondary contacts of the guest. This feature enables the operator to notify primary or secondary contacts of the arrival of the guest, if the person the guest is visiting is not available.

- 1 **Enable Primary or Secondary Contacts** - Check this option to allow the operator to enter additional Contacts.

Other

This section contains the table refresh timer and the color indicators for the status of the guest. The guest information on the Guest Pass System main window gets refreshed based on this timer. The different colors indicate the status of the guest badge i.e. valid, about to expire and expired.



- 1 **Table Refresh Timer** - Enter the number of minutes to specify the refresh interval of the guest pass record in the main window. You can enter the number either using the up and down arrows or manually.
- 2 **Guest Access Status Colors** -The status of the guest's access expiration date and time can be easily identified through the colors used. The user will be able to customize the status colors used to indicate this access expiration. The user can select different colors for valid, about to expire and one that has already expired.
 - a) **Valid Guest Access** - Click on the expand button to open the color palette. Select a color to indicate a valid access guest record. In the Guest Pass System main window, all the valid records will be displayed in the color you choose here.
 - b) **Days in Advance to Indicate Expiration** - Enter the number of days in which you want the system to change the **About To Expire Guest Access** field color.
 - c) **About to Expire Guest Access** - Select a color to indicate the badge that is going to expire soon.
 - d) **Expired Guest Access** - Select a color to indicate an expired guest badge.
 - e) **Maximum Visits Allowed by a Guest** - Set the maximum number of visits a guest can have. Once the guest's number of visits reaches the maximum number allowed, he/she cannot be signed in again without resetting the value here. This value can be reset through the **Guest Administration** part of the Guest Pass Settings.

Guest Pass Locations

In the Guest Pass System, Location refers to the site where the Guest Pass Workstation resides. Administrators can add, delete, modify or select a location using this tab. The Global Location is a factory set location which cannot be deleted. You may modify the name, Timezone and Guest Pass Setting that is attached to it. The Global location should be used if you want to view the guest information at every location. The Guest Pass System displays Guest records that are added in the Global Location, as well as the Location that is currently being viewed.

Each Guest Pass Workstation is linked to a Location and each Location is linked to a Setting. The changes that are made to a Guest Pass Setting with in a Location immediately take effect on the Guest Pass workstation.

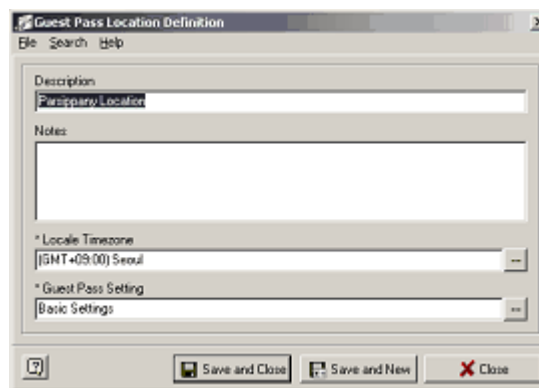
Note: Default Location is a factory set location and the user cannot edit or delete it. However, the user can still modify the description and notes filed of the factory set location.

The number of **Guest Locations** defined in the system is controlled through a security key (dongle). The system is shipped with only one factory set location (global location) and by default the maximum number of additional locations allowed in the system is zero. The user needs to install a dongle to have additional licenses to define new locations.

Note: Locations other than the Default/Global Location cannot be verified (via dongle security key) without a connection to the SP. Therefore, users cannot Add and Sign In new Guests in other Locations when the Guest Pass System cannot communicate with the SP. The Add Guest Wizard will inform users that the current Location is invalid when this occurs. Connection status is also displayed in main screen title bar. All other Guest Pass functionality and transaction writing is unaffected by lost SP connections.

Defining a Location

- 1 Click on **Guest Pass Locations** tab located at the Guest Pass Settings grid window.
- 2 Click on the + sign to open the **Guest Pass Location Definition** window.



- 3 Enter a description for the new location in the **Description** field. Type in the notes associated with it in the **Notes** field.
- 4 Select the time zone for the location. Click on the expand button to choose a time zone.

- 5 Select a **Guest Pass Setting** that the new location is going to use.
- 6 Click **Save and Close** to save the new location definition. Click **Save and New** to save and create a new location. If you click **Close** a confirmation message is displayed asking you to save the changes.

Defining a workstation

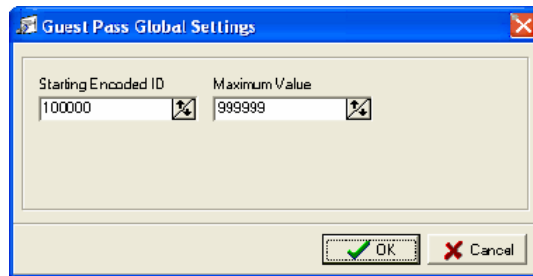
You can define any computer as a Guest Pass Workstation. You cannot select a computer that is already a Guest Pass Workstation. While defining a workstation you need to attach it to a Guest Pass Location. This feature is very important because the workstation will be using the Guest Pass Settings attached to this Guest Pass Location.

- 1 Click on the **Guest Pass Workstations** tab in the Guest Pass Settings window.
- 2 **Workstation** - Select the Location of this Workstation. The Workstation will use the Settings of the selected Location.
- 3 **Guest Pass Location** - Select the Location of this Workstation. This workstation will use the settings of the selected location.
- 4 **Badge Printer** - Select the **Enabled** check box to enable badge printing. Click on the expand button to specify the badge printer. The Guest Pass System will automatically choose this printer for printing badges.
- 5 **Label Printer** - Select the **Enabled** check box to enable label printing. Click on the expand button to specify the label printer. The Guest Pass System will automatically choose this printer for printing labels.
- 6 **Portrait Capture Device** - Enabling this option allows the operator to capture an image when adding a guest or upon signing them in. Using the drop down menu, select the Portrait Capture Device that you are going to use for image capturing. While adding a guest the device you choose here should be available for image capturing.
 - a) **From File** - The system opens the default Portrait folder (C:\Schlage\Data\Portraits)for you to choose the portrait.
 - b) **Twain Device** - The operator can acquire an image from a twain device i.e. a scanner or digital camera.
 - c) **Flashbulbs MV** - The operator can capture a picture using Flashbulbs MV.
- 7 **Signature Capture Device** - Enabling this feature allows the operator to save the digital signature of the guest and use it for verification of identity or reference. Using the drop down menu, select the signature capture device. The Guest Pass System will automatically use the device or method you selected here to capture the guest's signature.
 - a) **From File** - The system opens the default Signature folder (C:\Schlage\Data\Signatures)for you to choose the signature.
 - b) **Twain Device** - The operator can acquire an image from a twain device i.e. a scanner or digital camera.
 - c) **Schlage SMS**- A signature pad can be connected to the COM port to capture digital signatures.
- 8 **Enrollment Reader** - If this option is enabled, while defining area access for the guest and issuing a credential, the specified enrollment reader can be used to retrieve the **Encoded ID** of the badge. Here, you will select the enrollment reader that you are going to use. Click on the expand button to choose a reader from the list.

Global Settings

These settings will be applicable to all the Guest Pass Systems that are run on the same server. You can set the Encoded ID start position and the maximum value that can be used for an Encoded ID using the Global Settings option.

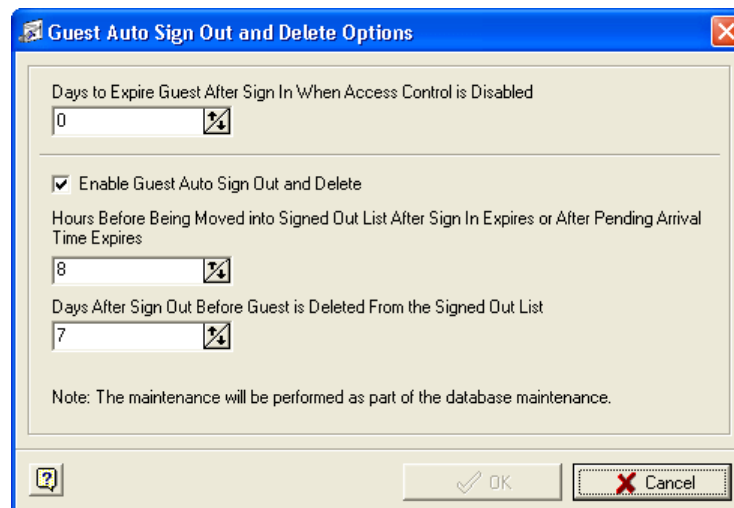
- 1 Select **Tools>Global Settings**. Set the Starting Encoded ID position and the maximum value. You can enter the value manually or use the up and down arrows.



Auto Sign-out options

The following options allow the user to set the different options such as deleting a guest record once the access rights are expired etc.

- 1 In **Guest Pass Settings**, select **Tools>Guest Auto Sign Out and Delete** options.



- 2 On the **Guest Auto-Sign Out and Delete Options** window, the following options are available:
 - a) **Days to Expire Guest After Sign In When Access Control is Disabled** - The guest record will expire exactly after the number of days set here once Access Control (Guest Settings Definitions>Access Control) is disabled. Enter the number of days in the field manually or using the up and down arrows.

- b) **Enable Guest Auto-Sign Out and Delete** - Select this check box to enable the options available under this section.
- c) **Hours Before Being Moved into Signed Out List After Sign In Expires or After Pending Arrival Time Expires** - The guest record, after it has expired from either the Signed In list or the Pending Arrival list, will be moved to the Signed Out list in the Guest Pass System exactly after the number of hours set here. If the value is set to zero (0), the guest will be signed out immediately after his/her access rights expire.
Example (1): A guest is signed in and the system generates an automatic expiration time of 11:59pm. The guest then does not sign out when they leave. If the **Hours Before Being Moved into Signed Out List After Sign In Expires or After Pending Arrival Time Expires** field has been set to 8, then eight hours after 11:59pm the guest record will be moved from the Signed In List to the Signed Out List.
Example (2): A guest record is in the Pending List for a 3:00pm appointment. The guest never arrives. If the **Hours Before Being Moved into Signed Out List After Sign In Expires or After Pending Arrival Time Expires** field has been set to 8, then eight hours after 3:00pm the guest record will be moved from the Pending List to the Signed Out List.
- d) **Days After Sign Out Before Guest is Deleted From the Signed Out List** - Once the guest record is in the Signed Out List, the guest record will be deleted after the number days set here.

The obsolete records are deleted from the database as a part of the maintenance job performed by the Database Maintenance Utility.
- e) Click **OK** to save the changes.

Guest Pass System

CHAPTER 46

Introduction

This chapter discusses the functions and characteristics of the Guest Pass System. The Guest Pass System module is used to create guest records and store their information in the cardholder database. Once your Guest Pass Settings are configured appropriately, you can start creating the guest record.

Note: Guest records can be created and maintained in various stages, from Pending and Unauthorized to Signed Out. This chapter illustrates three options for adding new guest records.

Overview

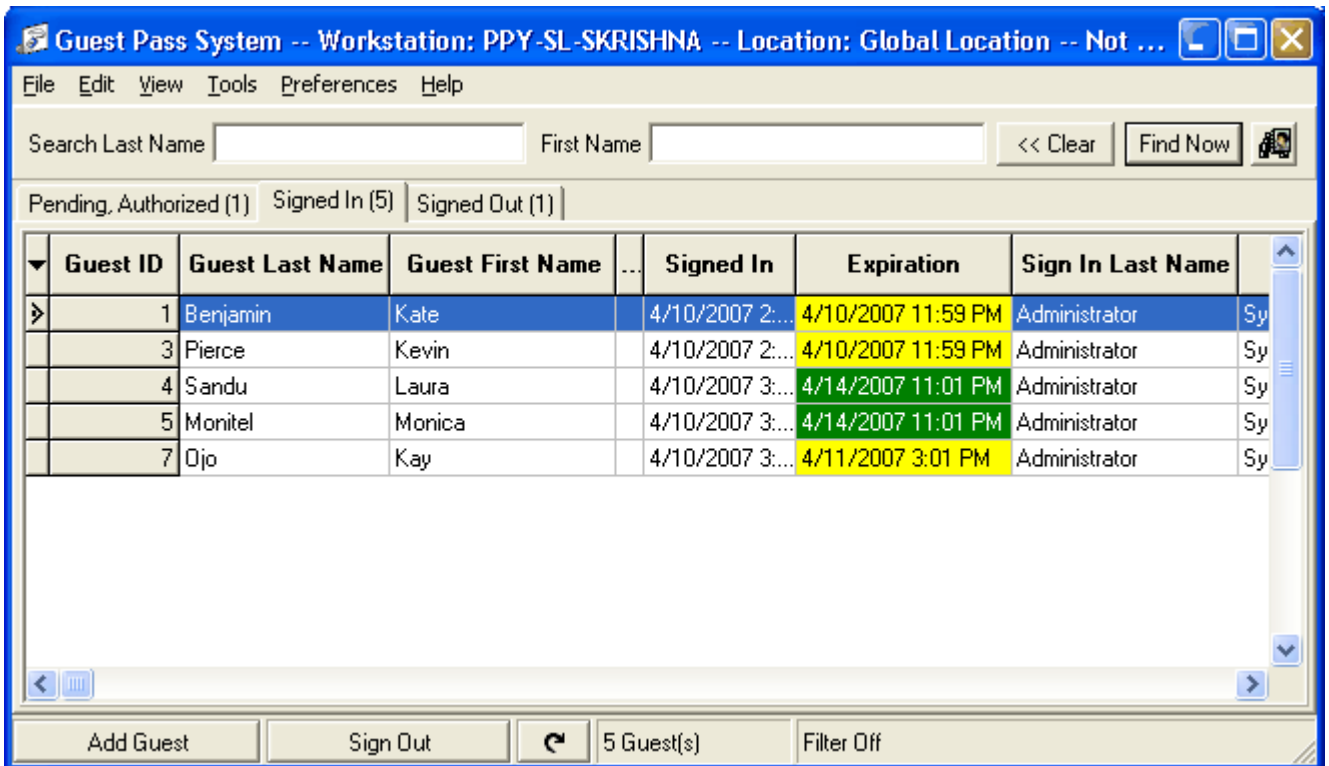
The main screen of the Guest Pass System module consists of the menu, search, task bars, tool bar and three tabs named **Pending Guests**, **Signed In** and **Signed Out**.

If you have created any User Defined Fields, those will be displayed in the main window of the Guest Pass System. When you define the fields be sure to select the option *Guest Pass Only* or *Both* in the UDF Editor program if you want those fields to appear in the Guest Pass System.

Color Schemes

Depending on the colors set in the Guest Pass Settings, in the Signed In tab, the fields for valid guest badge, about to expire badge, and expired badge will be indicated using different colors. These colors are customized by the user in the Guest Pass Settings.

Date and time fields are set to green for the current day, yellow for within 24 hours, and red for expired.



Green indicates a valid guest badge, yellow indicates an about to expire guest badge and red indicates an expired guest badge

Creating Guest Records

Note: The **Guest Pass System** requires **Area Sets** (not only areas) to be defined in order to add guests in the system.

Option 1

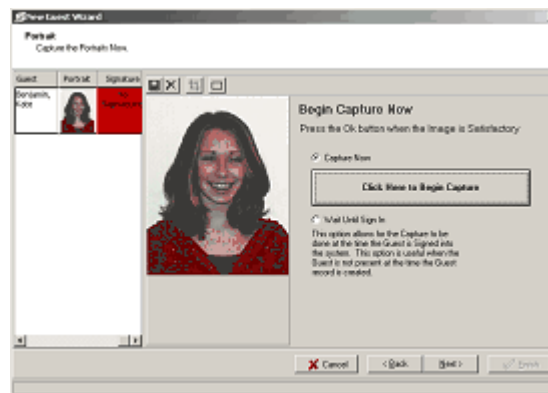
This section of the document is written based on the assumption that the steps for adding, authorizing signing in a guest happen sequentially. The system is capable of handling all three steps at the same time.

Adding Portraits to a Badge or a Label

- 1 In the **Portraits** window, press the **Click Here to Begin Capture** button to capture an image of the guest. Image can be captured from a file or through a TWAIN device or FlashbusMV.

Note: If you have not selected **Enable Portrait Capture** (Guest Pass Settings>Portrait Capture> Enable Portrait Capture) you can skip this section. You can choose to **Wait Until Sign In** when adding a pending guest. If you are issuing only labels go to step 14 to select a label layout.

- a) In the Guest Pass Settings, if you have set the *Default Image Capture Device* as **From File**, when you press the **Click Here to Begin Capture** button, your Portraits folder is displayed. You can select the required image from the folder.
- b) Select the appropriate image and click **Open**. The image is added to the window.



- 2 If you have set the *Default Image Capture Device* as **From TWAIN Device**, you need to select the device you are going to use for image capturing. Select the device and proceed with the process.
- 3 If you have set the *Default Image Capture Device* as **From FlashbusMV**, make sure that the Flash Bus camera is connected at the workstation. See Flash Bus user's manual for further details.

Editing the Image

The Guest Pass System is equipped with a collection of editing tools that you can use to modify images that are added. Once you insert the image to the window, the 4 buttons on the top of the window allow you to edit the image.

- a) **Cropping Rubber Band** - This tool allows you to select a portion of the image. Click on the tool to activate it. A rectangular rubber band appears on the image. This is the selection border. Click and drag the rectangular rubber band to place it over the desired portion of the image. Click on the edges to expand your selection. When you are satisfied with your selection click on the **Crop Image** button.
- b) **Crop Image Button** - After making your selection click on this tool to crop the image. The Guest Pass System is equipped with an **Image Enhancement Utility** program which enables the user to improve the quality of the image. To make this option available, you need to enable this option in the **System Manager Settings**.

In the **System Manager Settings**, click on **Schlage Image Settings**.

In the **General Image Settings**, select **Automatic Image Enhancement Utility**.

- 4 If you enable this feature, when you click on the **Crop Image** button the Image Enhancement Utility window will be displayed. You can adjust the brightness and contrast of the photograph using the **Decrease** and **Increase** buttons. When you are satisfied with the enhancement, click on the appropriate image and it will be inserted in the **Capture Image** window automatically.
 - a) **Cancel Changes** - This button allows you to cancel the changes that you have made to the image.
 - b) **Save Button** - Click on this button to save your changes.
- 5 Click **Next** on the **New Guest Wizard** to continue with the **Add Guest** process.

Add a Guest

- 1 You can begin adding a guest into the system in two different ways.
 - a) Click the **Add Guest** button located on the bottom of the Guest Pass System main window.

OR

 - b) From the Guest Pass System main screen select the **File>Add Guest** menu option.
- 2 In the following step select the type of guest entry. You can choose to sign in the guest now or later. If you enable the **Always Sign In When Allowed** option (Guest Pass Settings>Authorization Options>Sign In Question) and grant operator permissions, you can skip this step.
 - a) Select the first option if you wish to sign in the guest now. The user must have the rights to authorize guests.

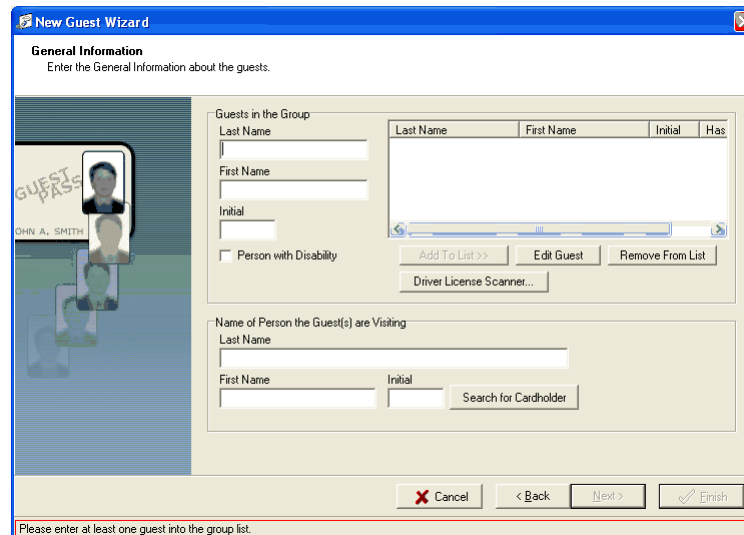
Note: If you choose not to sign in the guest now your guest record will appear in the pending guest section.

- b) Select the second option if you do not want to sign in the guest when you create the guest record.
- c) If you have Read/Write privileges to the Guest Pass System, you can select **Yes** or **No** to authorize the guest now.

Note: If you enable the *Always Authorize When Allowed option (Guest Pass Settings>Authorization Options>Authorization Question) and grant operator permissions, you can skip this step.*

- d) Click **Next** to continue, or **Cancel** to abort the process.
- 3 The Guest Pass System provides you the ability to add the guests as a group. In Guest groups, Access Control information such as expiration date and Areas will be common for all the guests in the group.

- 4 Next, enter the names of the guest.



- Enter the name of each guest and click the **Add to List** button. If you want to edit any guest name, select it and click on **Edit Guest**. To remove any guest from the list click on **Remove from List**.
- If the guest is a disabled person, select the **Person with Disability** check box.
- You can also enter the information about guests by choosing the **Driver's License Scanner** button. In order to have this option you need to fulfill the following requirements.

Driver's License Scanner requirements

Guest Pass Software Version 3.4

Our software supports the Scanshell 800 scanner model. This scanner is available through Ingersoll-Rand Security Technologies.

The scanner must be connected to a USB port directly connected to the computer and cannot go through a USB hub because of power requirements. If the scanner is connected to a USB port that does not provide enough power for the scanner, it will not function correctly.

In New Hardware Wizard, you need to use the option to **SELECT A LOCATION** for the driver files and browse to the Scanshell folder on the Guest Pass Installation CD.

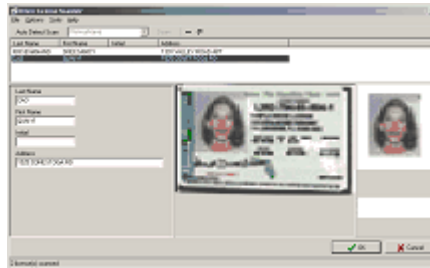
Note: Prior to scanning a license for the first time, you need to calibrate the scanner using a calibration sheet. The scanner will not function properly without this.

- Select the **Driver's License Scanner** button. The **Driver's License Scanner** window is displayed. The scanner scans driver licenses and extracts the textual information from the driver license into Guest Pass software.

Note: If the **Automatic Page Feed Detection** option is enabled in the Driver's License Scanner window (Options>Automatic Page Feed Detection), the user can scan a license without using the Driver License Scanner Dialog. The option is enabled by default. The process is as follows:

- The user must be on the General Information page of the **New Guest Wizard**. The user then must place a license in the Scanshell scanner. The scanner will automatically begin the scan and process the license. Once this is complete, the new guest will automatically appear in the wizard guest group list with required information from the license.

- 7 This dialog allows the scanning of driver's licenses and keeps the data of each scanned license during a session. You can scan as many licenses as you want before closing the dialog.



- 8 You can either select the **Auto Detect Scan** option or the **Scan** button. The Auto Detect Scan button performs a license scan and automatically detects the state. The Scan button performs a license scan using the state selected in the combo box to the left of the button. A state must be selected to use this button. The last state selected will be saved when the dialog is closed and reopened.
- 9 Once you select the appropriate button for scanning, calibrate the scanner using the calibration sheet (Tools\Calibrate Scanner: The scanner must be calibrated the first time it is used for it to work.) Now insert the driver's license to the scanner. The scanning may take a few seconds. When a license is scanned, the dialog attempts to extract the data from the license and fills in the mapped cardholder fields with it.

Note: All fields that have been mapped show up in this window, including fields mapped to cardholder fields that the current user does not have permissions to. In this case, the New Guest Wizard will not allow these fields to be saved or seen depending on the rights of the current user.

- 10 Minor errors can occur during the scan. To ensure data integrity, the user can modify the data if the extraction was not 100% correct. First select the guest, then make necessary changes to any of the mapped license fields.
- 11 The bottom middle pane will show the actual license that was scanned. This is useful to make sure the license scanned properly. If it does not look right, the data extracted from it probably will not be correct, either.
- 12 The bottom right pane holds the portrait and signature extracted from the license. A few states, including New Jersey, Oregon, and Virginia, do not support signature extracting.
- 13 The status bar displays the number of licenses scanned and being held in memory for the session.
- a) Enter the name of the person the guest is visiting and click **Next** or click on **Search for Cardholder** to choose a cardholder name from the database.
- 14 Next, enter additional details for each guest in the **Extended Information** page. The user defined fields are displayed here. Click on each guest in the left side of the dialog to enter unique information per person. For fields which may be common for all guests in the group, you may enter the data and then right-click in the field to **Apply to All Guests**.
- 15 In the following window, click **Select Cardholder to Find** and enter the names of the primary and secondary contacts of the guest. The people specified here may be notified of the guest's arrival in the event the person to be visited is unavailable.

Note: If you have not selected the **Enable Primary or Secondary Contacts** (Guest Pass Settings> Contacts> Enable Primary or Secondary Contacts) window in the Guest Pass Settings, this step will be skipped.

- a) Click **Next** to continue, **Back** to go back or **Cancel** to cancel the process.
- 16 In the following window enter the instructions you want be displayed while signing in and/ or signing out the guest.

Note: If you have not selected the *Enable Instructions option (Guest Pass Settings> Instructions> Enable Instructions)* you can skip this step.

- a) Click **Next** to continue, **Back** to go back or **Cancel** to cancel the process.
- 17 In the next window, enter the e-mail addresses of the people that you want to notify regarding the arrival and departure of the guest.

Note: If you have not activated Enable E-Mail in the E-Mail settings (Guest Pass Settings>E-Mail>Enable E-Mail) this step will be skipped.

- a) Press the **Add Address button** to add the address and **<Remove Address>** to remove the e-mail addresses.
- b) Click **Next** to continue, **Back** to go back or **Cancel** to cancel the process.
- 18 In the following window enter the expected arrival date and time of the guest. The drop down arrow in the date field displays the calendar. Use the up and down arrows to adjust the time.
- a) Click **Next** to continue, **Back** to go back or **Cancel** to cancel the process.
- 19 Next, select the expected arrival location of the guest. Click on the expand window to see all the locations defined in the system. Select the Use the Location of this Guest Pass System, if the guest is expected to arrive at that location.
- a) Click **Next** to continue, **Back** to go back or **Cancel** to cancel the process.
- 20 Next select the Access Time for the guest.

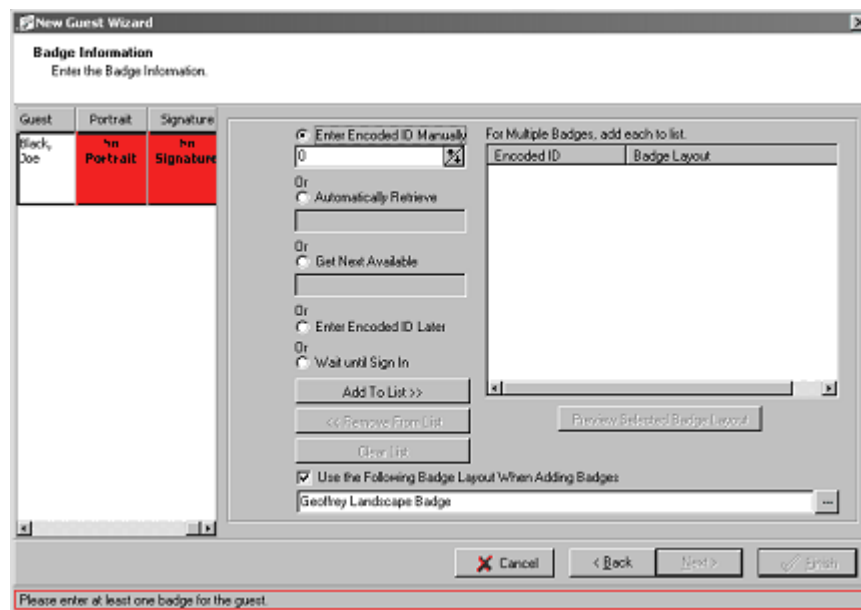
Note: If you are using Automate Area Access option (Guest Pass Settings Definition>Access control) with default Access Template, steps 10 &11 will be skipped.

- a) **Use a Guest Access Template** - Select the radio button to enable the option. Click the expand button to select a template.

Note: The Access Templates are defined in the Guest Settings module.

- b) **Manual Entry** - This option allows you to either select the access time in hours or enter the date and time of access expiration. If you choose to use the hourly option, select the **For** radio button and enter the number of hours in the empty field next to it.

- 21 To enter the date of access expiration, select the **Until** radio button and choose the date using the drop down calendar and use the up and down arrows to indicate the time. You can also enter the data manually into the fields.
- 22 **Guest Access Timezone** - Click the expand button to choose a timezone.
- 23 You can also specify access expiration as a particular time of the day that the guest is signed in. Select the **At** radio button and specify the time.
- a) Click **Next** to continue, **Back** to go back or **Cancel** to cancel the process.
- 24 Next select the **Area Sets** that the guests will have access. Select the **Add Area Sets** button. If you wish to delete any of the area sets from the list, select the record and click **Remove Area Sets**. In order to delete the entire list click **Clear List**. Click **Next** to continue, **Back** to go back or **Cancel** to cancel the process.
-
- Note:** If you have selected an Area Access Template in the previous step, this step will be skipped.
-
- 25 The next step is to enter the credential information of the guest. Enter the encoded ID of the badge you are assigning to the guest. If you are adding multiple guests, you need to assign at least one encoded ID per guest.



- a) There are several options for adding Encoded ID, as follows: Enter manually, Automatically Retrieve using a Schlage Enrollment Reader, Get Next Available id from a range defined in Settings, Enter Encoded ID later or Wait Until Sign In.

Note: To retrieve the encoded ID number automatically, you must have the enrollment reader defined in the Guest Pass Workstation Definition form of the Settings module. To use **Get Next Available** option, you have to set the starting and maximum values for the encoded id in the Guest Pass Settings>Tools>Global Settings section.

- b) Press **Add To List** button to add the encoded ID or **Remove From List** to remove it from the list. The ID that you added and the badge layout you've selected will be shown in the list on the right side of the window. If you are using a default badge layout, the layout you selected in the Settings will be displayed in the Badge Layout list. If you are not creating badges the field displays *Not Required*.

- c) There is also an option to **Use the Following Badge Layout When Adding Badges**. This feature streamlines the process of applying the same layout when adding or signing in a group of guests. The last selection chosen will be saved until changed by the user.

Note: If you have selected **Default Badge Layout>Always Use the Default Badge Layout** (Guest Settings>Badging>Default Badge Layout>Always Use the Badge Layout Selected Below) this option will be disabled.

- d) Click **Next** to continue, **Back** to go back or **Cancel** to cancel the process.

Adding Signature to the Badge

- 1 If you have enabled **Signature Capture Requirement** you will be asked to add a signature to the badge or label you are creating.

Note: If you have not enabled signature capture (Guest Pass Settings>Signature Capture>Enable Signature Capture) this step will be skipped.

- a) Click on the **Click Here to Begin Capture** button to capture a signature.
 - b) Using the device you have selected in Guest Pass Settings, capture a signature. If you have previously captured signatures stored in a file and your **Signature Capture Setting** is **From File**, you will be prompted to select from the Signature folder by default or browse to your designated storage location to capture the guest signature.
- 2 If you are creating labels select a label layout for the guest.

Note: If you have not activated **Enable Label Printing** (Guest Pass Settings>Label Printing>Enable Label Printing> and if you have already selected a default label layout, this step will be skipped.

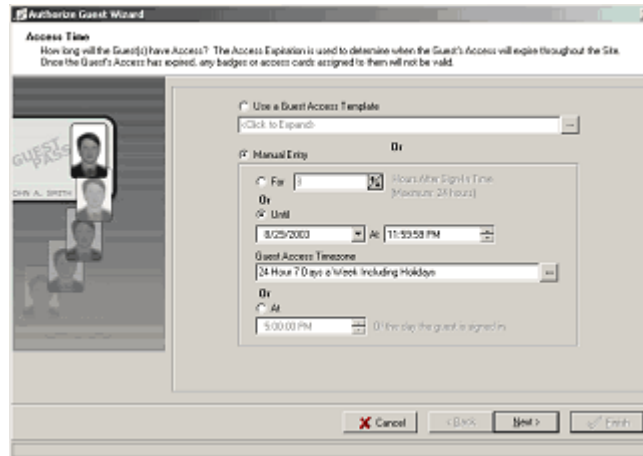
- 3 If you are adding an image to the label, follow step 12 on page .
 - a) Press the **Preview Selected Layout** to preview the badge layout. If you are satisfied with the layout you selected, click **OK** and then select **Next** to proceed to the Create Guests window.
- 4 A confirmation message is displayed saying that you are going to add a new guest into the system, click **Finish**.
- 5 A new guest record is created in the Guest Pass System in the pending list. You can view the guest record by clicking the **Pending Not Authorized** tab located in the Guest Pass System main window.

Authorize a Pending Guest

After adding a guest into the system, he/she should be authorized by somebody who has authorization privileges. If the operator has authorization privileges, he can authorize the guest once he creates the guest record. The following are the instructions to follow to authorize a guest.

- 1 Click the **Pending Not Authorized** tab in the Guest Pass System window.
- 2 All the unauthorized guest records which are not Signed in are displayed. Click and select the guest record you want to authorize.
- 3 Click on the **Authorize** button located at the bottom of the Guest Pass System window.

- 4 In the next window, select the guest's access expiration time. Using the up and down arrows you can either select the expiration time by hours or select a particular date and time. Select a time zone. The guest will have access to the Areas only during this time interval. You can also choose a specific time on the day the guest is signed in.



- a) Click **Next** to continue, **Back** to go back or **Cancel** to cancel the process.
- b) If you are not using Access Templates, in the **Access Time** window you may use the **Access Template** or **Manual Entry** options. Select the Area Sets you want to assign the guest and click **OK** to continue. You can see the guest record now in the Pending, Authorized tab of the main window. Click **Finish**.

Sign In a Guest

Once the guest is authorized you can sign him into the system. The following are the steps to sign in a guest.

Note: If you define a reader as "Sign In" reader, the system will automatically sign in the guest when he/she swipes the card on that reader. Refer to System Manager to know more about defining readers.

- 1 Click on the **Sign In** button located at the bottom of the Guest Pass window.
- 2 If the option **Require Image Verification on Sign In** (*Guest Pass Settings>Image Verification>Require Image Verification on Sign In*), you will be prompted to verify the portrait and signature. Click **Next** when you are done with the verification. If you want to capture the portrait or signature again click on **Click Here to Begin Capture**.
- 3 This next step is the **Badge Information** window. You can verify or modify or enter new information if it is needed (this step is already described previously in the chapter). Click **Next**. to proceed to the Instructions page.
- 4 The instructions to follow before sign in are displayed.

Note: If you have not enabled **Automatically Pop-up Instructions** (*Guest Pass Settings>Enable Instructions>Automatically Pop-up Instructions*) this step will be skipped.

- 5 The **Confirm** dialogue box is displayed. Click **OK** to print badge or label.
- 6 The system will sign in the guest and update the guest record in the Guest Pass System main window.

Option 2

This section of the document is written based on the assumption that the steps for adding, signing in and authorizing a guest happen at the same time.

Add, Authorize and Sign In a Guest

- 1 Follow step 1 under “**Option 1-Add a Guest**”.
- 2 Next, select the first option i.e. *Create Guest Record and Sign the Guest(s) in Now*. Click **Next**. You should have authorization privileges to sign in a guest.

Note: See Glossary of Terms for further details on authorization privileges.

- a) Click **Next** to continue **Back** to go back **Cancel** to abort the process.
- 3 Follow steps 3, 4, 5, 6 and 7 under “Option 1- Add a Guest”.
 - 4 Next, follow step 3 and 4 under “Option1-Authorize a Pending Guest”.
 - 5 Next, follow steps 10 to 16 under “Option1-Add a Guest”.
 - 6 A progress indicator displays each portion of the process. If you have elected to use the Guest Settings options to Cancel Before Badge and/or Label Printing, a Print dialog will be displayed for each guest record. This will allow the operator the choice to print each badge and label immediately or not. The Guest Pass system creates a new guest record under the **Signed In** list. You can view the guest record by clicking **Signed In** located in the Guest Pass System main window.

Option 3

This section of the document is written based on the assumption that the steps for adding a guest, and authorizing a guest happen at the same time. But the guest is signed in at a later time.

Add and Authorize a Guest

- 1 Follow step 1 under “Option 1-Add a Guest”.
- 2 The **New Guest Wizard** opens. Select the type of entry. Choose the option **Create Guest Record(s), but do not sign the Guest(s) in Now**. Select Yes to the question, *Will you be the authorizer of the Guest?*
- 3 Next, follow step 3 to 9 under “Option 1-Add a Guest”.
- 4 Next, follow step 3, and 4 under “**Option1-Authorize a Guest**”.
- 5 Follow, step 10, 11, 12, 13, 14, 15 under “Option 1-Add a Guest”.

A new guest record is created in the Guest Pass System under the pending section. You can view the guest record by clicking the **Pending** button located on the Guest Pass System main window. You can also see that the guest record you created is authorized.

Sign In a Guest

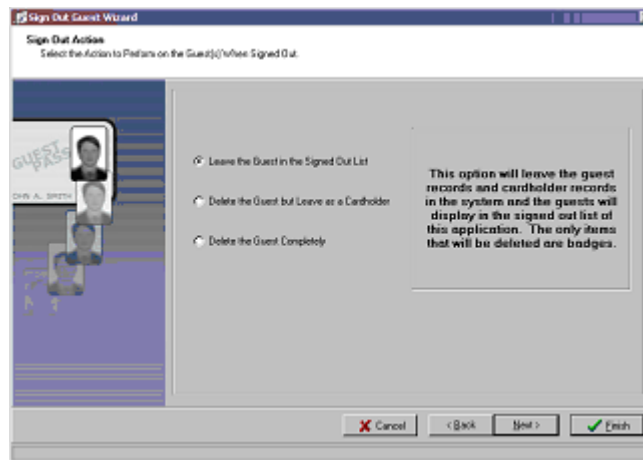
Follow steps under “Option1- Sign In a Guest”.

Sign Out a Guest

Follow these steps to sign out a guest from the system.

Note: If you define a reader as “Sign Out” reader, the system will automatically sign out the guest when he/she swipes the card on that particular reader. Refer to Ch 3-System Manager to know more about defining readers.

- 1 Click and highlight the guest record that you want to sign out from the system on the Guest Pass System's main screen.
- 2 Right click on the guest record and select Sign out Guest from the menu or click the **Sign Out** button. The **Sign-Out Guest Wizard** begins.



- 3 There are three options available to perform on the guest record while signing out.
 - **Leave the Guest in the Signed Out List** - This option will leave the guest records and the cardholder records in the system and the guests will be displayed in the Signed Out list of the application. The guest badges are deleted.
 - **Delete the Guest but Leave as a Cardholder** - This option will delete the guest records, but guest will remain as cardholders in the database. These cardholder records can be viewed and modified using the **Cardholder Definition** application. The guest badges are deleted.
 - **Delete the Guests Completely** - This option will delete the guest record completely. All the information including badges, access control information, e-mails etc. will be deleted permanently and cannot be recovered.
 - The Cardholder's portrait and signature are displayed.
- 4 The **Sign Out Action** window comes next. Sending you screen shots of all three options with descriptions from the Sign Out wizard - you may want to use one shot and just use the explanations from the other two.
- 5 The system will handle the guest record according to the **Sign out Action** selected and update the main screen with the changes.

Reset Guests to Pending

Signed Out guests may be reverted to Pending status for future return visits. The Guest Pass System provides operations that quickly perform the conversion for you.

Follow these steps to reset signed out guest records to pending guest records.

- 1 From the **Signed Out** tab on the main screen select the guest(s) you wish to Reset.
- 2 Click the **Reset to Pending** button at the bottom of the main screen or right click on the record and from the menu, select **Reset Guest to Pending**.

Note: You can use the option to **Edit Guest Information** prior to reset the guest record to pending.

- 3 Now you may either reset the guest(s) to **Pending** or reset and **Sign In Now**. All the steps documented under the section Adding a Guest are executed here for verification purposes. You can choose to use the same information or can modify the data according to the user's specific requirements.
- 4 The system will create a pending or signed in guest record and update the guest record window.

Editing the Guest Information

In the Guest Pass System main window the new guest name is added. Once the guest is added, you can review or modify most of the guest information you have added by double or right clicking on the guest record on the main screen or you can perform this through the edit menu.

Guest Information On: Kate Benjamin

General Information | Authorization Settings | Instructions on Guest | E-Mail Addressing


Guest

Last Name: Benjamin

First Name: Kate Initial:

☐ Person With Disability

Portrait



Description

Name of the Person the Guest is Visiting

Last Name: Kirshnanand

First Name: Sandya Initial: <- Select Cardholder...

Expected Date and Time

Date of Arrival: 4/10/2007

Time of Arrival: 2:38:11 PM

Name of Authorizer

Last Name: Administrator

First Name: System

Visit Count

1

Expected Location

Global Location

OK Cancel

Description of tabs

- 1 **General Information** - Select this tab to see general information regarding the guest. This includes the name of the guest, name of the person the guest is visiting, the arrival date and time, portrait, signature and expected location. The Authorizer's name is also displayed and label printing also may be performed from this tab.
- 2 **Extended Information** - Any additional information added through the User Definable Fields is displayed here.
- 3 **Contacts** - This tab allows you to view or modify the primary and secondary contacts of the guest. Clicking on the **View Detailed Cardholder Information** allows you access the cardholder information.
- 4 **Authorization Settings** - This tab allows you to modify the authorization settings of the guest. The **Re - Authorize this Guest** button allows you to re-authorize the guest and modify the access expiration date and time.
- 5 **Instructions on Guest** - You can view and modify the instructions added while signing in the guest.
- 6 **E-mail Addressing** - You can view and modify the e-mail addresses you have added while adding the guest into the system.
- 7 **Badge Assignments** - This tab displays the information of the badges that are currently assigned to the guest. The buttons allow you to preview and/or print badge and assign Encoded ID.

Delete a Guest Record

The Guest Pass System allows you to delete a signed out guest record completely. You can also choose to leave the guest as a Cardholder.

You can access the delete function in two ways.

- 1 Click on the guest record you want to delete.
- 2 Right click on the record or go to the **Edit** menu and select **Delete Guest Completely**.
- 3 The system will delete the records and update the guest record window.

Search for a Guest

Guest Pass System is now enabled with a more precise search feature to assist users in finding the guest records easily. The user can search for guest records under **Signed In**, **Pending** and **Signed Out** tabs separately. When the user runs a search, the system displays only those records that match the criteria specified by the user.

The system also puts a wildcard automatically at the end of the words typed in the Last Name and First Name fields. When the user clicks the **Find Now** button, the system return all the records that starts with the letters in the search fields. If you want to expand your search criteria, you can put a% (percentage) sign in front of the letters you typed in and the system will return all the guest records that contain the letters you used.

Guest records are displayed in yellow if any of the following conditions occur:

- A guest is signed in at a different location
- A guest is signed out at a different location
- A guest is pending and expected at a different location

Last Name	First Name	Initial	Activation Date	Expiration Date	Cardholder ID	EncodedID	StampedID	Raw Card Data	No
Benjamin	Carolyn		4/10/2007	12/31/2199	6				
Benjamin	Kate		4/10/2007	4/10/2007	5				
Monitel	Monica		4/10/2007	4/14/2007	9	8907			
Ojo	Kay		4/10/2007	4/11/2007	11	5678			

Advanced Find

The user can search for specific guest records based on Guest Fields, Credential Criteria, Activation and Expiration Date, Area Access, and Location.

Search for a Guest

Using **Advanced Find**, you can build the search criteria by selecting appropriate entries from the drop down list box and entering specific values in the value field. You have to select a specific field name, condition and a specific search value.

The Advanced Find feature uses Boolean logic to create complex and highly precise searches. Boolean logic uses three connecting operators (NOT, AND OR) to narrow or broaden a search or exclude a term from the search.

The Advanced Find feature enables the operator to customize the search functions and save them for later use.

The saved search criterion is displayed only for the operator who defined it.

Guests can be searched using cardholder fields (like first name, last name etc.), Credential criteria or activation and expiration date.

Click on the Advanced Find tab located on the top of the Search window.

- 1 The **Advanced Find of Guests** window opens.
- 2 Click on the **Guests Fields** tab to search for guests by field name.
- 3 Define your search criteria.
 - a) If you want to search for Guest ID = 10, you need first select the left parenthesis from the list box.
 - b) Parenthesis can be used to create nested search clauses. Using the parenthesis one can override the standard order of priority (left to right) for each Boolean statement in the search.
 - c) Select Guest ID as the Field Name.
 - d) Select equal to (=) as the condition.
 - e) Enter the value as 10.
 - f) Provide the closing parenthesis at the end.
 - g) When you are satisfied with the criterion, click the **Add to List** button. If the criterion is not valid, it is displayed in red under the **Where Clause** section. When the criteria becomes valid the font color changes to black.
 - h) If you would like to specify additional search conditions, you can select AND/OR from the list box.

E.g. If you want to search Guest IDs less than or equal to 10 and last names with the letter "K" and Guest IDs greater than or equal to 20 and last names with the letter "D", define the search criteria as follows.

```
((Cardholder ID>=10) AND (Last Name LIKE%k%)) OR ((Cardholder ID>=20) AND (Last Name LIKE%d%))
```

When you run the search you will get the records corresponding to your search criteria. The **Guest Search and Select** window displays the search results.
 - i) Once you have defined the criteria click **File>Save**.
 - j) Add a description to your search and click OK.
- 4 The new search will be saved and accessed under the **Advanced Find** button.
- 5 You can also search for Guests using Credential Criteria, Activation and Expiration Date, Area Access and Locations.

Use of Wildcard

The Advanced Search feature provides ways to select certain guest records without typing complete information. **Schlage SMS** allows the use of wildcard (more formally known as *metacharacters*) to stand for one or more characters in a guest record. A wild card is a value entered into a query field that represents any other value and is usually used when exact values are not known. The users can do partial match searches by using the% (percent sign) as a **wildcard**. Within the search criteria, a user can type the% character before or after their search text as a wildcard

E.g. Entering%re will return all the last names that end with the letters “re”. By using the wildcard in the beginning, the user is requesting the system to find all values that ends with “re” and ignore preceding characters.

Burner

Craggier

Kaiser

Entering %er% will return all the last names that contain the letters “er”.

Anderson

Berner

Creager

Kaiser

Roberts

Sathers

Wildcard has a very flexible capability to help users identify specific information based on limited or partial search information. One thing to note; however, this capability can result in very large query results if misused.

Anderson

Berner

Creager

Kaiser

Roberts

Sathers

Credential Criteria

- 1 In order to search for a badge based on the badge information you need to specify one of these options.
- 2 First select the search type. Here you need to specify whether you need to run the search based on Badge ID or Encoded ID. Next select the range of the search. You need to specify a beginning ID or ending ID.
Or
- 3 You can also search for guests based on the badge creation date. Specify a range of date and time.
Or
- 4 The third method of searching is by the date and time that the badge was printed. Here you need to enter a beginning and ending date and time.

- 5 Select the Include Retired Badges option, in order for the search to contain retired badges.
Or
- 6 If you select the option **Find All Active Guests with No Active Badge Criteria**, all the active guests defined in the system are displayed regardless of any criteria.
- 7 Click **Find Now**.

Activation and Expiration Tab

- 1 Select the **Activation and Expiration** tab.
- 2 Choose the option **Activation Between** to find the Guests based on their Area Access Activation date or select **Expiration Between** to find the records based on the expiration date.
- 3 Now specify the range of date (starting date and ending date).
- 4 Click **Find Now**.

Area Access

This option allows you to find the records based on the Area Access.

- 1 Select the **Area Access** tab.
- 2 Click on **Add Areas**. Highlight and select the area records on the **Search for Areas** window based on which you want to search for guest records. You may Remove Areas from the search criteria, also.
- 3 Click **Find Now**.

Locations

- 1 Select the **Locations** tab.
- 2 You can search for **Expected, Signed In or Signed Out guests** by Location. Make your guest status selection by clicking the radio button.
- 3 Click **Add Locations** and highlight and select the locations in the **Search for Guest Locations** window. Click **OK**. **Remove Locations** can be used to modify the criteria, or Clear Locations to remove all selections. Click **Find Now**.

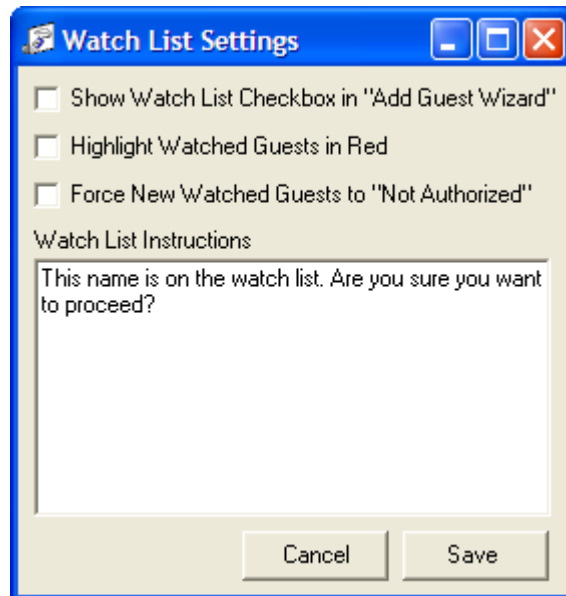
On Watch List

Guest Pass has a new "On Watch List" feature. This feature allows you to designate any new guest record as "On Watch List". When a guest is added to Guest Pass, if they have the same first and last name as a guest record marked as "On Watch List", a warning dialogue will open. From this dialogue the operator can view the "On Watch List" record to determine whether the guest attempting to sign in is the guest on the watch list. If so, the operator can then choose whether or not to sign the guest in.

Note: If you do not wish to use this feature simply uncheck the **Show Watch List Checkbox in "Add Guest Wizard"** option in Watch List Settings.

Watch List Settings

To configure the Watch List Settings, open Guest Pass and go to **Tools>Watch List Settings**.

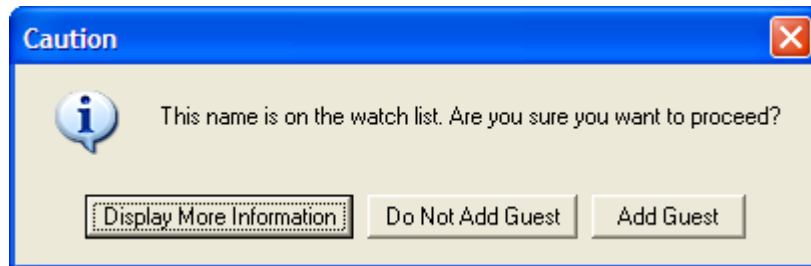


Note: these settings are only enabled if the user has Administrative permission to Guest Pass.

- **Show Watch List Checkbox in "Add Guest Wizard"** - Checking this option enables the "On Watch List" option in the Add Guest Wizard. If this is not checked it will not be possible to add guest records to the watch list.
- **Highlight Watched Guests in Red** - Checking this option will highlight any "On Watch List" guest records in red.
- **Force New Watched Guest to "Not Authorized"** - Checking this option will force any guests marked as "On Watch List" to the Pending, Not Authorized tab. It will be impossible, without turning off this feature, to authorize, sign in, or sign out these guest records.
- **Watch List Instructions** - the text in this field will appear in the warning dialogue in Add Guest Wizard if someone attempts to add a guest name identical to one on the watch list.

New Guest Wizard

- **On Watch List** - Check this option to mark a guest record as On Watch List.
- **Description** - Enter any notes or descriptions here.
- **Caution** - This dialogue appears if an operator attempts to add a new guest record that has the same first and last name as a record marked "On Watch List". It has three options:



- **Display More Information** - Will open the On Watch List guest's information window.
- **Do Not Add Guest** - Will close the dialogue and not add the guest record.
- **Add Guest** - Will close the dialogue and add the guest record.

License Field Cross Reference

CHAPTER 47

Introduction

The **License Field Cross Reference** application allows the user to map the fields on a driver's license to the existing cardholder fields. It is used in the Guest Pass System to fill in the cardholder fields by scanning a guest's driver's license. First Name, Last Name, and Initial are automatically mapped fields and cannot be changed by the user.

These fields display in the light blue factory set color. The user can create user defined fields to match with the driver's license fields and retrieve information by scanning the guest's driver's license.

Our software supports the Scanshell 800 scanner model. This scanner is available through IR Security Technologies.

The scanner must be connected to a USB port directly connected to the computer and cannot go through a USB hub because of power requirements. If the scanner is connected to a USB port that does not provide enough power for the scanner, it will not function correctly.

Accessing the application

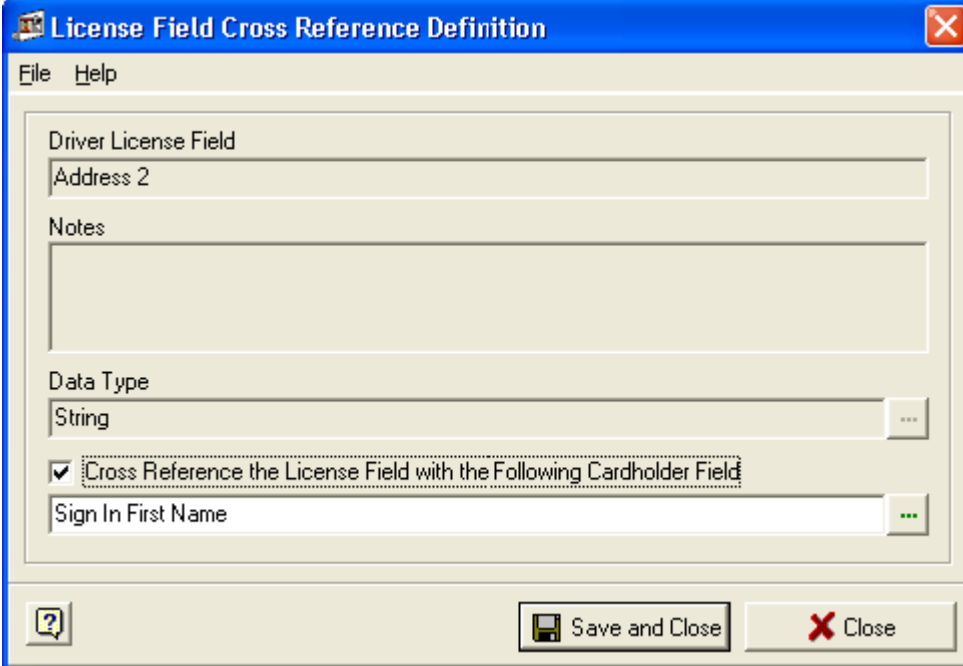
- 1 Open the System Launcher by double clicking the Schlage SMS icon on your desktop or select **Start>Programs>Schlage SMS>Schlage SMS**.
- 2 The login window, opens. Enter your user ID and password.
- 3 In the **System Launcher** window, double click on **License Field Cross Reference** icon.

Mapping

Follow these steps to create a cardholder field that has cross reference to a driver's license field.

- 1 For example, create a user defined field called "Address" using the UDF Editor program.
- 2 Open the License Field Cross Reference program You can all the driver's license fields listed on the left column.
- 3 Click on the driver's license field you want to link with the cardholder field. For this example we are using the Address field.

- 4 The **License Field Cross Reference Definition** window allows the user to map the driver's license field with a existing cardholder field



The image shows a software window titled "License Field Cross Reference Definition". It has a menu bar with "File" and "Help". The main area contains several fields: "Driver License Field" with the value "Address 2", a "Notes" text area, "Data Type" with the value "String", and a checked checkbox labeled "Cross Reference the License Field with the Following Cardholder Field". Below the checkbox is a field containing "Sign In First Name". At the bottom, there are three buttons: a help icon, "Save and Close", and "Close".

Driver License Field	Address 2
Notes	
Data Type	String
<input checked="" type="checkbox"/> Cross Reference the License Field with the Following Cardholder Field	
	Sign In First Name

- 5 Select the check box **Cross Reference the License Field** with the following cardholder field.
- 6 The field **Data Type** displays the type of the field.
- 7 In the following field, select the UDF that you want to link with the driver's license field. A list displays all the user defined cardholder fields. Your selection appears in the field, and the list closes.
- 8 Choose **Save and Close** to save the record.

LockLink Import Wizard

CHAPTER 48

Introduction

The **LockLink Importer Wizard** (referred to as "Importer" throughout the rest of this chapter) enables users to import data from LockLink 7 and LockLink Express databases into the **Schlage SMS** database. Before starting the import process, the Importer prompts the users to choose the source (LockLink 7 or LockLink Express) of the import. It also provides functionality to create online credentials while creating offline credentials, match LockLink user's credentials with credentials that are already present in the SMS database, and import user groups as cardholder categories. Additionally, the Importer allows users to replace leading zeros with nines while importing "PIN only" or "Plus PIN" credentials. These features are explained later in this chapter in detail.

Important Note: The LockLink Import Wizard (LLImport.exe) replaces existing LockLink 7 Importer and LockLink Express Importer utilities. The users should now use the LockLink Import Wizard to import Locklink Express and Locklink 7 databases into Schlage SMS. The existing Importer utilities will not work with the new release.

The following data is imported into the **Schlage SMS** database:

- Users/People (known as Cardholders in **Schlage SMS**)
- Time zones
- Holidays
- Doors (Offline Locks)
- Auto unlocks (automatic overrides) associated with doors
- Access Records
- Buildings and access profiles (applicable only to LockLink 7)
- Magstripe Template

Note: Magstripe templates are imported only from LockLink Express databases. If you are importing a LockLink 7 database, Magstripe template must be set up manually in **Schlage SMS**.

While importing data, the Importer creates a new Cardholder Category and an Area Set (in System Manager) containing all the People/Users records and Doors. An Area is created for each door with a caption identical to the door's caption.

All the People records are grouped into a Cardholder Category called "LL_Import_CurrentDate_Category" and all the doors are grouped into an Area Set called "LL_Import_CurrentDate_AreaSet". The "CurrecntDate" refers to the time when the data is imported.

Limitations

The Importer does not import the following records:

- Operator / Login privileges
- Reports
- Audits (the end user may wish to keep the LockLink Express/LockLink 7 installation for reporting purposes)
- Any data related to Campus Lock including campus plans, etc.
- Magstripe Template - If you are importing data from LockLink 7, Magstripe templates should be setup manually in **Schlage SMS** using System Manager or Card Format Editor prior to importing. LockLink Importer imports Magstripe templates from LockLink Express.

Imported Data Types

The following table describes how different data types are imported from LockLink Express and LockLink 7 databases to Schlage SMS.

Data Types	LockLink 7	LockLink Express
Users/People	All LockLink 7 Users are imported as cardholders in Schlage SMS along with any Magstripe, proximity, iButton, or PIN only credentials. Credentials such as E-Bolt, ProxIF, Campus, and RSI hand credentials are skipped by the Importer. A log file is created containing the information about the skipped records. All pre-existing Cardholders in the Schlage SMS will be left untouched.	All LockLink Express People records are imported as cardholders in Schlage SMS along with any Magstripe, proximity, iButton, or PIN only credentials. Credentials such as E-Bolt, ProxIF, Campus, and RSI hand credentials are skipped by the Importer. A log file is created containing the information about the skipped records. All pre-existing Cardholders in the Schlage SMS will be left untouched.
Time Zones	The Importer imports timezones defined in the SmarTime portion of LockLink 7 creating new Timezones in Schlage SMS as needed. It also imports the auto unlock schedules (known as Automatic Overrides in Schlage SMS) defined in SmarTime creating new timezones.	The Importer imports seven (7) timezones defined in the SmarTime portion of LockLink Express creating new Timezones in Schlage SMS as needed. It also imports the auto unlock schedules (known as Automatic Overrides in Schlage SMS) defined in SmarTime creating new timezones.
Holidays	The Importer imports all holidays defined in SmarTime into the Holidays section of System Manager.	The Importer imports all holidays defined in SmarTime into the Holidays section of System Manager.

Data Types	LockLink 7	LockLink Express
Doors (Offline Locks)	<p>The Importer creates a door in Schlage SMS for each door type (Campus Lock and CM Lock) found in LockLink 7. E-bolt, Handkey, Interflex, CL, Rabbit Controllers and mechanical doors are not imported. The Caption of the door in Schlage SMS is set to what the door was named in LockLink 7, and the Description field is set to blank. If there are multiple doors with the same name, the LockLink 7 Door ID is appended to create a unique caption.</p> <p>The Importer retains the association between a door and time zones. During the import process, a newly imported door is associated with whatever time zones it was associated within LockLink 7. However, the utility only associates up to fifteen (15) time zones with a door in this manner; the reason is that Schlage SMS uses one of the sixteen(16) allowed slots for “always” (a factory set timezone). If sixteen (16) timezones are associated with a door in LockLink 7, the last timezone is skipped and an entry is noted in the error log.</p> <p>The Importer creates a brand new area for each door with a caption identical to the door’s caption.</p>	<p>The Importer creates a door (Area) in Schlage SMS for each door type (Campus Lock and CM Lock) found in LockLink Express. E-bolt, Handkey, Interflex, CL, Rabbit Controllers and mechanical doors are not imported. The Caption of the door in Schlage SMS is set to what the door was named in LockLink Express, and the Description field is set to blank. If there are multiple doors with the same name, the LockLink Express Door ID is appended to create a unique caption.</p> <p>The Importer retains the association between a door and time zones. During the import process, a newly imported door is associated with whatever time zones it was associated within LockLink Express. However, the utility associates up to seven (7) time zones with a door in this manner; the reason is that Schlage SMS uses one of the eight (8) allowed slots for “always” (a factory set timezone). If eight (8) timezones are associated with a door in LockLink Express, the last timezone is skipped and an entry is noted in the error log.</p> <p>The Importer creates a brand new area for each door with a caption identical to the door’s caption.</p>
Access Records	<p>All LockLink 7 access records that associate a credential with a door are imported into Schlage SMS. Access records that associate a credential to either an access profile or access profile group are ignored without logging. The Schlage SMS does not permanently associate access to a group.</p>	<p>All LockLink Express access records that associate a credential with a door are imported into Schlage SMS. Access records that associate a credential to either an access profile or access profile group are ignored without logging. The Schlage SMS does not permanently associate access to a group.</p>
Buildings and Access Profiles	<p>An Area Set is created for each building and each access profile. For each door that was part of a building or access profile, its newly created area is added to the appropriate set.</p>	<p>N/A</p>

Data Types	LockLink 7	LockLink Express
Magstripe Template	Magstripe templates must be set up in the Schlage SMS manually using System Manager or Card Format Editor.	Magstripe templates created in LockLink Express are imported to Schlage SMS and sets as template used for CM Locks in the system.

Importing LockLink Express Database

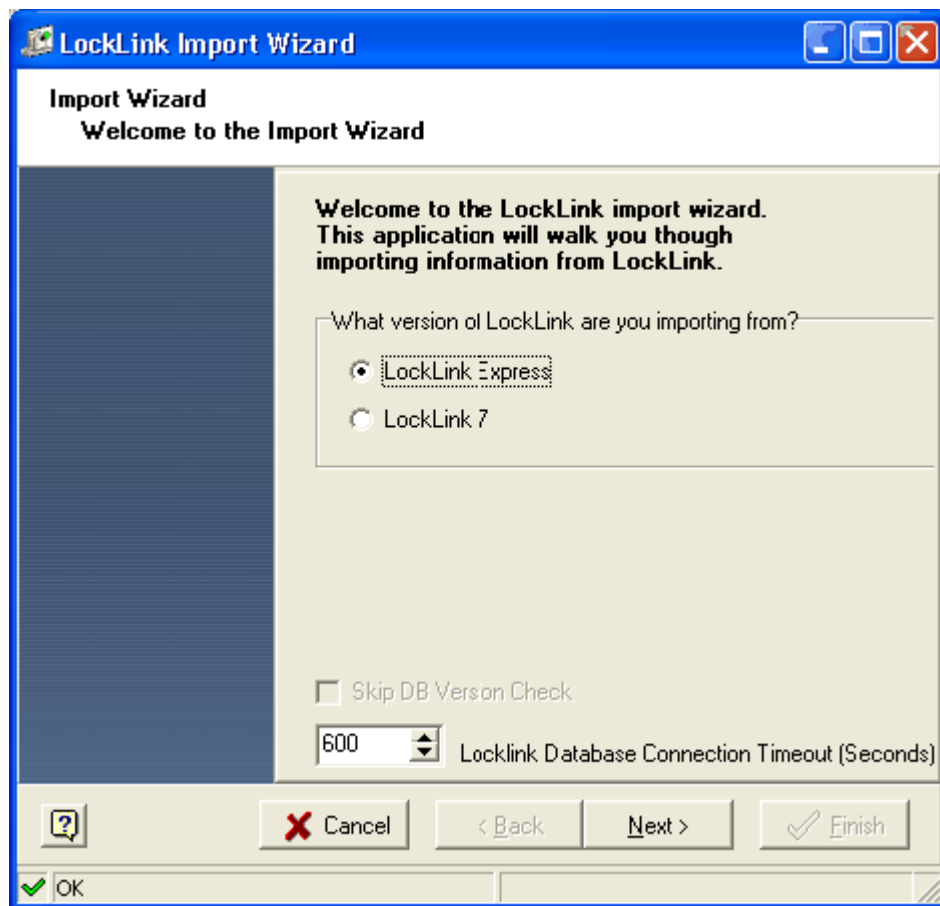
Pre-requisites for importing a LockLink Express file

- 1 The **Schlage SMS** version 5.3 must be installed before running the Importer, otherwise the Importer displays an error on startup and halt. The user should not enter any data into the database before running the Importer. If the same data has been partially entered by hand and then imported, it can lead to having duplicate records or information being omitted.
- 2 LockLink Express must be installed on the machine where the Importer will be run. If LockLink Express is not installed on any machine that runs **Schlage SMS** system, the **Schlage SMS** client can be installed on the source LockLink Express machine and the Importer can be run from that machine. Alternatively, LockLink Express can be temporarily installed on a machine that runs Schlage SMS, and the .lld file can then be moved from the original source to the machine. The file select dialog explained later in this chapter can be used to select that file for import.
- 3 LockLink Express must be closed before running the Importer.
- 4 If you wish to use the imported credentials at online locks, you need to set up appropriate card formats in the system prior to importing the cardholder records. The Card Format Editor program allows users to create custom card formats and select existing card formats. Refer to Chapter 03- Card Format Editor for more information on setting up card formats.
- 5 During the importing process, the LockLink Importer attempts to insert the credentials using the card formats currently selected in the **Schlage SMS**. If the Importer cannot find a card format that matches with a credential, it imports that credential only with the raw data, without deriving the Encoded ID. Such credentials can be used at offline locks, but will not function at online locks.
- 6 The database file you are importing must be set to read/write (not read-only). If the file is set to "read only", the Importer display "not a valid password" error message. Note that typically when a backup of a database is restored, the recreated file will be read-only. This must be changed to read/write prior to performing the import.
- 7 The file titled "SampleLLEImport.ips" must exist in the bin directory along with the executable itself. This file instructs the Importer how to interpret LockLink Express as a data source. If this file is missing or the version is outdated, the Importer displays an error message and aborts the import process.

Steps for Importing a LockLink Express File

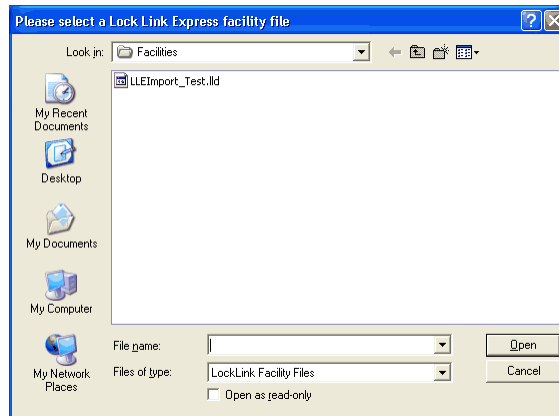
- 1 Go to **C:\Program Files\Schlage\Bin**. Double click **LLImport.exe** icon to start the Importer.

- 2 On the LockLink Import Wizard, select the **LockLink Express** radio button.

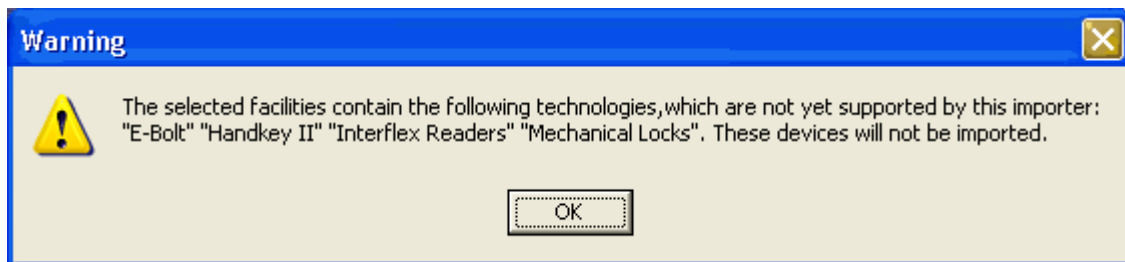


- a) **Skip DB Version Check** - If enabled, this option forces the system to skip the step that verifies the version of the Schlage SQL database. If the database version is below 5.3, the Importer displays an error message and halts the process. This option is not enabled for users.
- b) **LockLink Database Connection Timeout (seconds)** - The connection to the LockLink Express database will time out in the duration specified here. You can either enter the value manually or adjust it using the up and down arrows.
- c) Click **Next**.

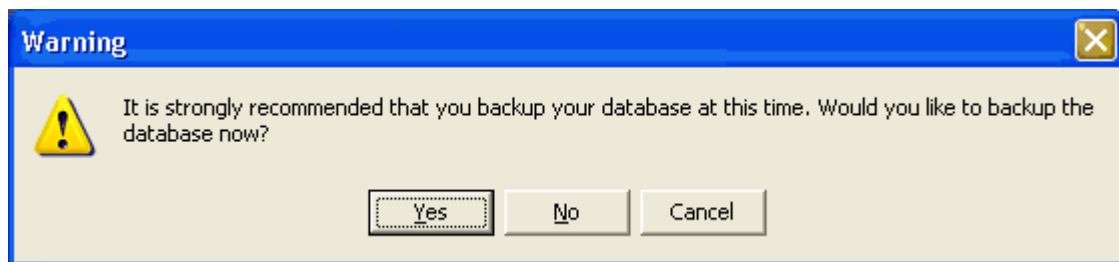
- Now, select a LockLink Express Facility file to import. By default, the Importer points to the "C:\Program Files\LockLink Express III\Facilities" folder where Facility files are usually found. The user must select a Facility file to continue. Click **Open**.



- If the importer finds any credential technologies not supported by the **Schlage SMS**, a message is displayed detailing which technologies will be omitted from the import. You have the option to cancel the import if this was not known prior to starting the import, or you may continue and import the other available information. If no unsupported technologies are used in the facility, this step is skipped. If no unsupported technologies are used in the facility, this step is skipped. Click **OK**.



- The **Backup Warning** screen is displayed recommending users to back up their Schlage SMS database.

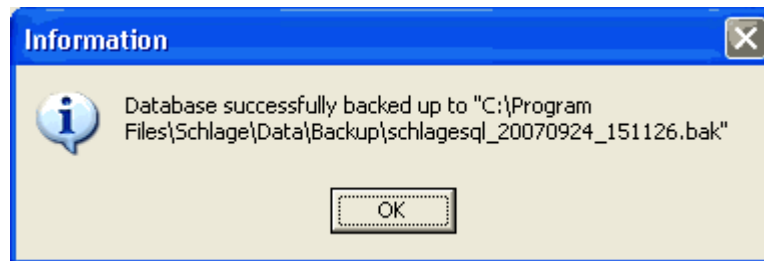


If the user chooses **Yes**, the utility will attempt create a current backup in the following location.

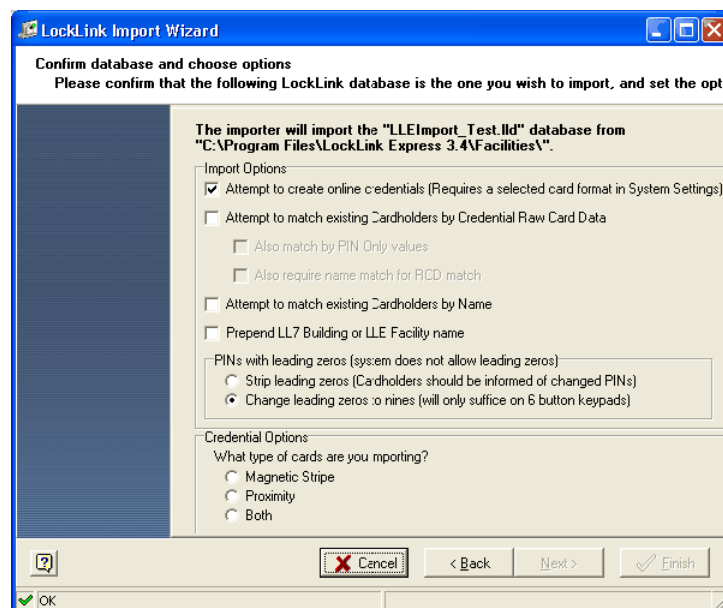
C:\Program Files\Schlage\Data\Backup.

The backup will work if the importer is run from a Schlage SMS client or server machine, but the backup file will always be stored on the server machine.

Once the database is successfully backed up, the following confirmation message is displayed. Click **OK**.



- 6 In the next step, the Importer confirms the LockLink Express database they wish to import. Also, the user can further customize the import by choosing the following **Import Options**.



- a) **Attempt to create online credentials (Requires a selected card format in System Settings)** - If this option is selected, during the import process, the Importer tries to create an online credential when an offline credential is created.

The Importer attempts to extract an online Encoded ID from the offline raw card data stored in the Lock Link database. If it is successful, it attempts to create an online credential at the same time it creates the offline credential.

The online Keypad ID is set to whatever the offline Keypad ID (aka "plus pin") is; however note that if the online reader does not actually contain a keypad, Keypad ID will not be created.

Online readers do not support functions (i.e. toggle, dogging, etc) at this time; all offline credentials are imported as regular online credentials, regardless of their functions. If there are multiple records corresponding to the same badge with different PINs for different functions, only one online credential is created with a Keypad ID equal to whichever function was added first in LockLink.

The system must have a valid card format defined for the importer to extract a valid online Encoded ID. For any credentials which do not have a valid and selected card format, or credentials which would cause an duplicate online record, the importer will make a log entry and skip the online credential creation but still attempt to create the offline credential.

- b) **Attempt to match existing Cardholders by Credential Raw Card Data** - if this option is enabled, the Importer matches newly imported cardholder records with records already present in the **Schlage SMS** database by raw card data.

Before inserting a new cardholder (known as "users" and "People" in LLE and LL7), the Importer checks if any of LockLink user's credentials (excluding PIN Only records) already exists in the SMS database. If so, it assumes that that LockLink user corresponds to the existing cardholder, and instead of creating a new cardholder, will import user's lock access, user groups, and credentials into the existing cardholder record. Existing demographic information (name, UDF, etc) and Lock/Area access records are left alone.

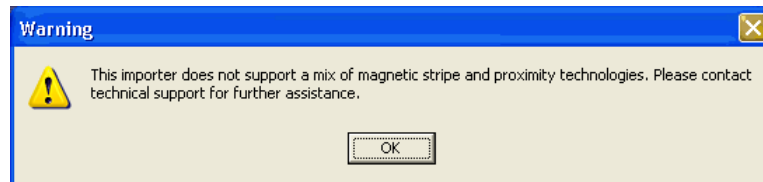
This feature is useful when importing multiple LLE facilities which contain overlapping cardholder populations, or when importing a LockLink data which contains credentials that have already been entered into **Schlage SMS** via Cardholder Definitions.

Operators should be careful that this does not erroneously assign information; for instance if credential 1234 has already been assigned to a cardholder named John Doe in SMS, but that same credential value 1234 was assigned in the LockLink database to a user named Mary Jane, Mary Jane will not be created by the import and her access will be assigned to John Doe instead.

- **Also match by PIN Only values** - If this option is enabled, the Importer checks if a user/people record with the same PIN Only credential exists in the SMS database. If one exists, the Importer will not create a new cardholder record. If this option is not enabled, the Importer will not try to match PIN Only records.
 - **Also require name Match for RCD match** - If this option is enabled, the Importer not only matches the credential data, but also the last and first name. Enabling this option avoids the potential mix up described above with John Doe and Mary Jane, but poses a different problem; if someone is entered as "John Doe" in LockLink, but as "Jonathon Doe" in SMS, they will not be matched if this option is enabled.
- a) **Attempt to match existing Cardholders by Name** - Enabling this option forces Importer to match newly imported cardholder records with records already present in the database by name.
- Before inserting a new cardholder (which are called "users/people" in LLE and LL7), the importer checks if any existing cardholder records have the exact same last and first name, and if so, imports that user's access, user groups, and credentials into the existing cardholder record. This is similar to the match by RCD option, except name rather than card number is used as the matching criteria. Operators should be careful, since misspelled names, and common names shared by several people (i.e. "John Smith") can cause erroneous import.
- b) **Prepend LL7 Building and LLE Facility Name** - If this option is enabled, the Importer prepends either the building name (LL7) or facility name (LLE) when importing new CM doors. This is useful in cases where there are multiple doors sharing the same name in LockLink. For instance, with this option turned on, if both "Building A" and "Building B" contain a door named "Room 123" in the source LockLink 7 database, they will be imported as "Building A - Room 123" and "Building B – Room 123" respectively. This is much clearer than the default behavior (with this option off), which creates two records called Room 123 with an automatically generated unique number at the end of each name in SMS.
- c) **PINS with leading zeros (system does not allow leading zeros)** - Importer now has selectable behavior to deal with leading zeroes.
- **Strip leading zeros** (Cardholders should be informed of changed PINs) - Unlike LockLink, SMS does not allow either "PIN Only" or "plus PIN" credentials to have a leading zero. Previous versions of the Importer, as well as the current version removes leading zeros when this option is selected. This can cause problems because the resulting number may be too short, or conflict with other numbers (for instance 012 would be changed to 12, which is too short for a pin, and 01234 would be changed to 1234, which could conflict with a pre-existing pin 1234.). In addition, it is problematic, because affected cardholders need to be informed that their PIN numbers have changed. In such cases, the following option can be used as an alternative method.

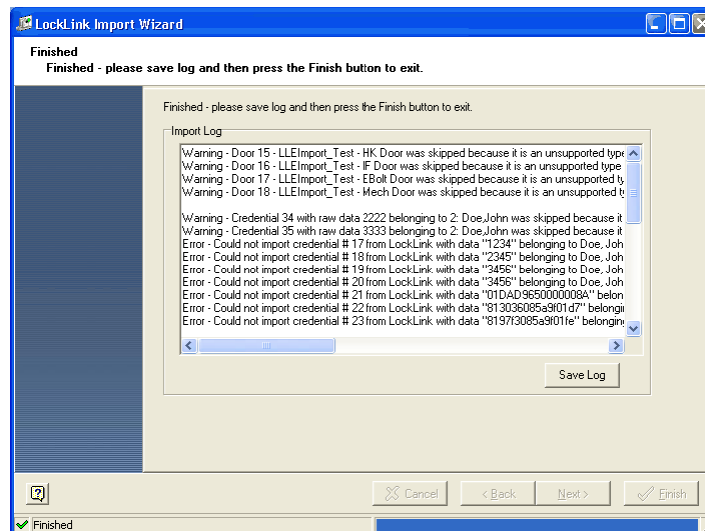
- **Change leading zeros to nines** - Enabling this option replaces any leading zero digit with a nine. (So 012 would change to 912, and 001234 would change to 901234). Since, on CM locks with 6 button keypads, nine and zero share a single button, this can be done without affecting the day to day usage of cardholders. However for CM locks with 12 buttons keypads, cardholders should be notified of their new PINs.
- a) **Credential Options** - Next, if the installation uses access cards (not only PIN and iButton), you are prompted to specify the types of cards (Magstripe and/or Proximity) that are being used. The reason for this is that the Schlage SMS differentiates between Magstripe and Proximity Cards whereas LockLink Express does not. The importer asks only the technology, but not the card format, and will attempt to use the selected formats already chosen in System Settings/Card Format Editor to derive the Encoded ID for each credential. If the Encoded ID for a given credential cannot be derived, a credential with null encoded ID is created.

Select the card type by clicking a radio button. Notice that the **Next** button is disabled until you select a card type. If you select the option **Both**, indicating a mix of both Magstripe and Proximity cards, the program will halt and the following error message is displayed.



- 7 The import process starts and displays the **Performing Import** window. The utility will go through a two stage process of reading the data and then applying scripts. The progress bar is incremented from empty to full twice as these two processes are completed. The user is prohibited from taking any action while this is going on, and the cursor is displayed as an hour glass. Upon successful completion, the **Finished** window is displayed. Click **Finish** to exit.

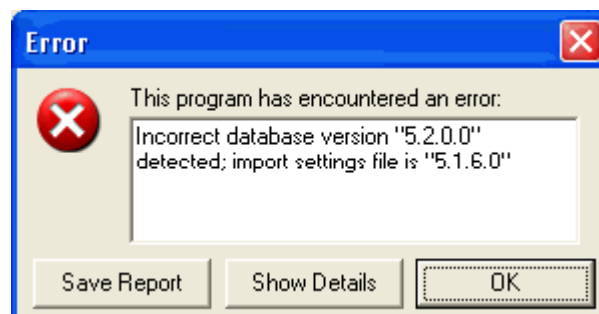
If any warnings or errors were generated by the process, a log will be displayed as shown below. Warnings indicate expected problems, such as records that were skipped because the technology is not supported by the importer (Interflex or mechanical locks, RSI Handkey credentials, etc.). Errors indicate things unexpected problems, such as a card whose data was incorrectly formatted or duplicate card numbers.



Importing LockLink 7 Database

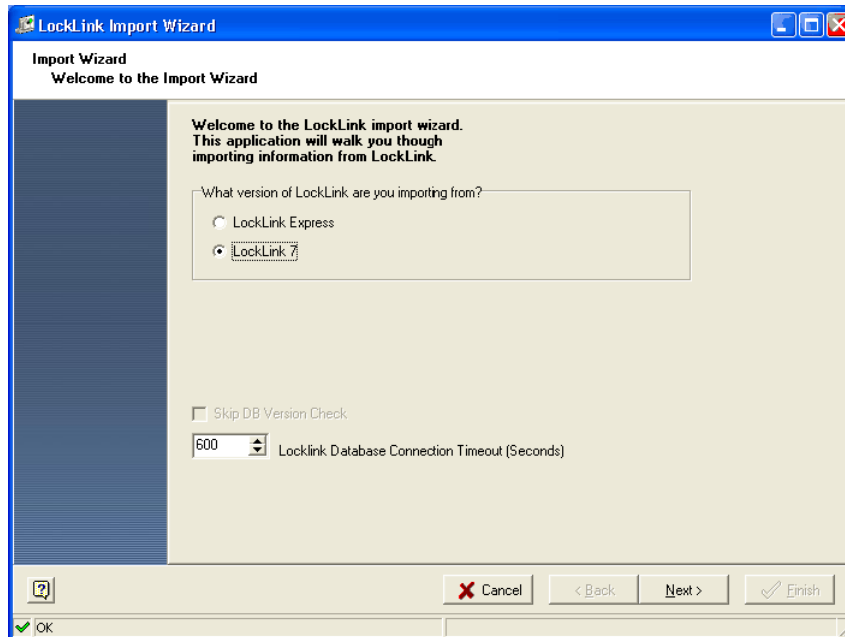
Pre-requisites for importing a LockLink 7 Database

- 1 The **Schlage SMS** Version 5.3 must be installed before running the importer. The importer must be run on Schlage SMS version 5.3, otherwise the Importer displays an error on startup and halt. The user should not enter any data into the database before running the importer. If the same data has been partially entered by hand and then imported, it can lead to having duplicate records or information being omitted.
- 2 The Lock Link 7.4.0.4 must be installed. Newer or older versions may or may not import correctly, depending on the nature and extent (if any) of differences in the database structure and usage for these versions.
- 3 The Importer can be run on any client or server machine in the **Schlage SMS**. LockLink 7 must be installed on the machine where the application will be run. If LockLink 7 is not installed on any machine that runs Schlage SMS system, then the Schlage SMS client can be installed on the source LockLink 7 machine and the importer can be run from that machine. Alternatively, LockLink 7 can be temporarily installed on a machine that runs Schlage SMS, and the.mde file can then be moved from the original source to the machine. The file select dialog explained later in this chapter can be used to select that file for import.
- 4 The database file you are importing must be set to read/write (not read-only). If the file is set to "read only", the utility will display "not a valid password" error message. Note that when a backup of a database is restored, the recreated file will be read-only. This must be changed to read/write prior to performing the import.
- 5 If you wish to use the imported credentials at online locks, you need to set up appropriate card formats in the system prior to importing the cardholder records. The Card Format Editor program allows users to create custom card formats and select existing card formats. Refer to Chapter 03- Card Format Editor for more information on setting up card formats.
- 6 During the importing process, the LockLink 7 Importer attempts to insert the credentials using the card formats currently selected in the Schlage SMS. If the utility cannot find a card format that matches with a credential, it will import that credential only with the raw data, without deriving the Encoded ID. Such credentials can be used at offline locks, but will be unusable at online locks.
- 7 Magstripe Template should be manually defined in Schlage SMS.
- 8 LockLink 7 must be closed before running LockLink 7 Importer.
- 9 The Microsoft Access file being imported should not be set to "read only". If the file is set to "read only", the application will display "not a valid password" error message.
- 10 The file titled "SampleLL7Import.ips" should be in the bin directory along with the executable itself. This file instructs the importer how to interpret LockLink 7 as a data source. If this file is missing or the version is outdated, the utility will display the following screen and abort the import process.



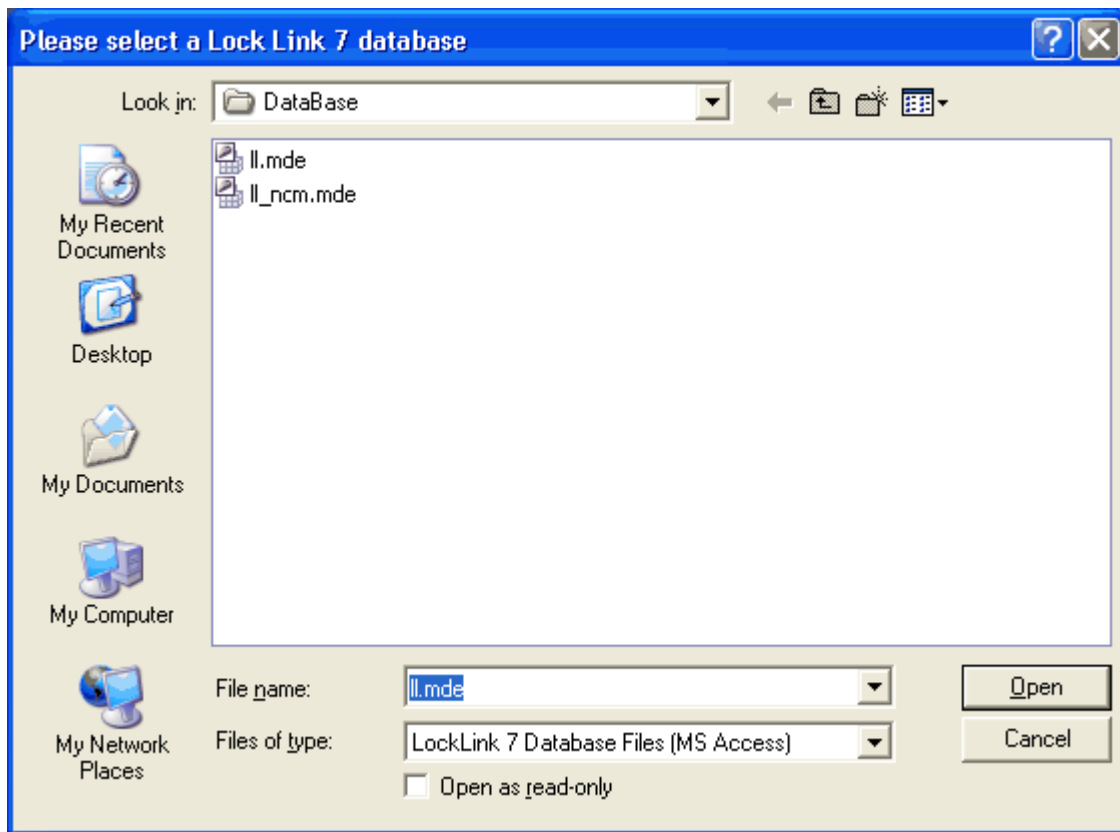
Steps for importing a LockLink 7 database

- 1 Go to **C:\Program Files\Schlage\Bin**. Double click **LLImport.exe** icon to start the Importer.
- 2 On the LockLink Import Wizard, select the **LockLink 7** radio button.



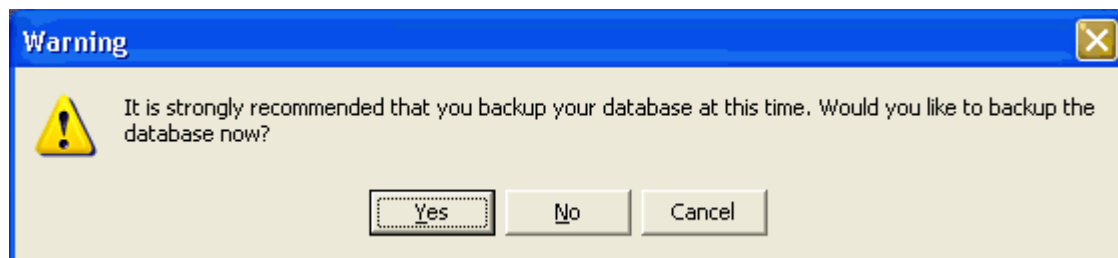
- a) **Skip DB Version Check** - Select this option to skip the step that verifies the version of the Schlage SQL database. If the database version is below 5.3, the Importer displays an error message and halts the process. This option is disabled for users.
- b) **LockLink Database Connection Timeout (seconds)** - The Importer attempts to connect to the LockLink Express database in the duration specified here. Once it passes the time specified, the database connection will timeout. You can either enter the value manually or adjust it using the up and down arrows.
- c) Click **Next**.

- 3 In the next step, the Importer prompts users to select a LockLink 7 database to import. By default, the Importer points to the "C:\Program Files\LockLink7\DataBase" folder where database files are usually found. The user must select a database file to continue. Click **Open**.



- 4 Next, The **Backup Warning** screen is displayed recommending users to backup their **Schlage SMS** database. If the user chooses **Yes**, the application attempts create a current backup in the following location.

C:\Program Files\Schlage\Data\Backup The backup works if the importer is run from a **Schlage SMS** client or server machine, but the backup file is always stored on the server machine.



Once the database is successfully backed up, a confirmation message is displayed. Click **OK**.

- 5 Next the Importer confirms the LockLink 7 database to be imported. Review this and choose the following settings appropriately to further customize the import.

- a) **Attempt to create online credentials (Requires a selected card format in System Settings)** - If this option is selected, during the import process, the Importer tries to create an online credential when an offline credential is created.

The Importer attempts to extract an online Encoded ID from the offline raw card data stored in the Lock Link database. If it is successful, it attempts to create an online credential at the same time it creates the offline credential.

The online Keypad ID is set to whatever the offline Keypad ID (aka "plus pin") is; however note that if the online reader does not actually contain a keypad, Keypad ID will not be created.

Online readers do not support functions (i.e. toggle, dogging, etc) at this time; all offline credentials are imported as regular online credentials, regardless of their functions. If there are multiple records corresponding to the same badge with different PINs for different functions, only one online credential is created with a Keypad ID equal to whichever function was added first in LockLink.

The system must have a valid card format defined for the importer to extract a valid online Encoded ID. For any credentials which do not have a valid and selected card format, or credentials which would cause a duplicate online record, the importer will make a log entry and skip the online credential creation but still attempt to create the offline credential.

- b) **Attempt to match existing Cardholders by Credential Raw Card Data** - if this option is enabled, the Importer matches newly imported cardholder records with records already present in the **Schlage SMS** database by raw card data.

Before inserting a new cardholder (known as "users" and "People" in LLE and LL7), the Importer checks if any of LockLink user's credentials (excluding PIN Only records) already exists in the SMS database. If so, it assumes that that LockLink user corresponds to the existing cardholder, and instead of creating a new cardholder, will import user's lock access, user groups, and credentials into the existing cardholder record. Existing demographic information (name, UDF, etc) and Lock/Area access records are left alone.

This feature is useful when importing multiple LLE facilities which contain overlapping cardholder populations, or when importing a LockLink data which contains credentials that have already been entered into **Schlage SMS** via Cardholder Definitions.

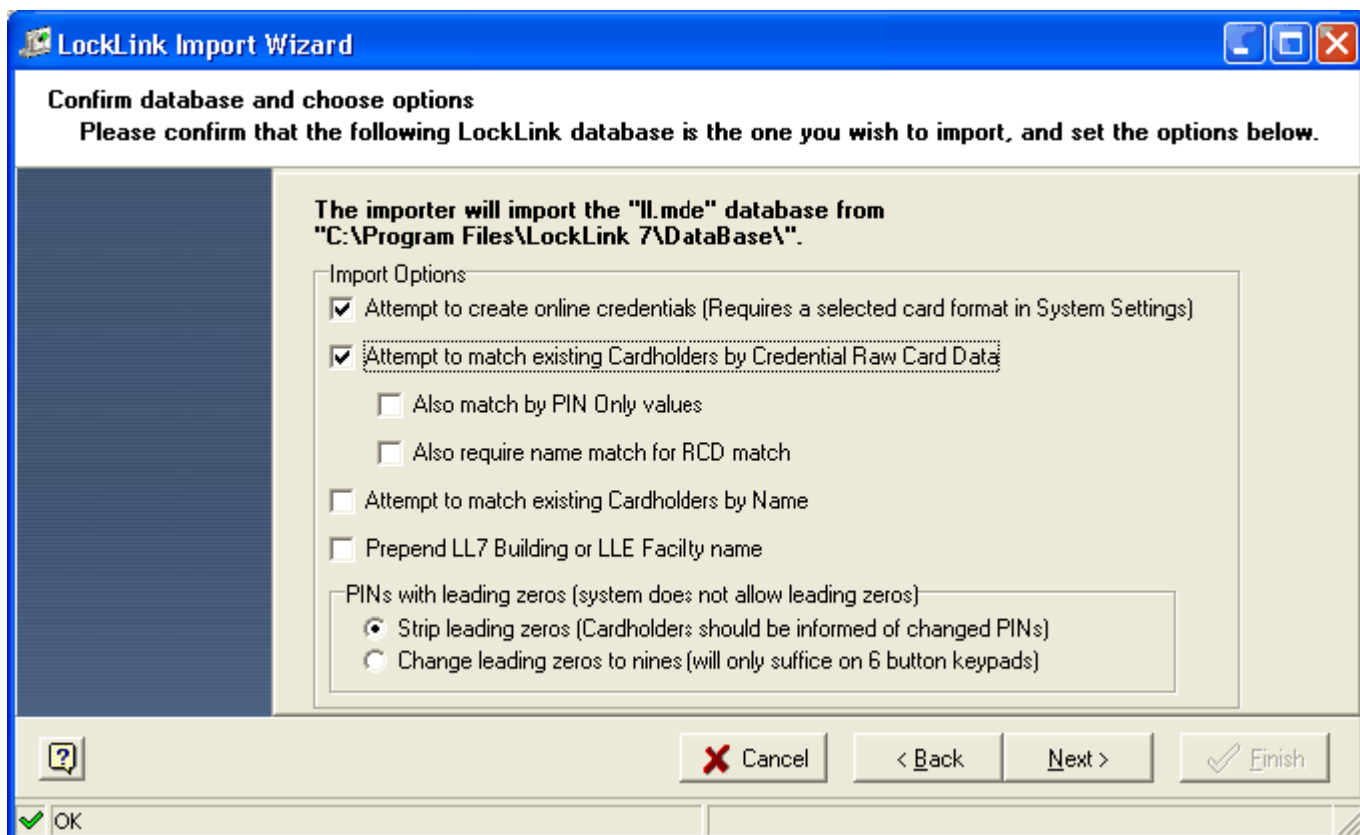
Operators should be careful that this does not erroneously assign information; for instance if credential 1234 has already been assigned to a cardholder named John Doe in SMS, but that same credential value 1234 was assigned in the LockLink database to a user named Mary Jane, Mary Jane will not be created by the import and her access will be assigned to John Doe instead.

- **Also match by PIN Only values** - If this option is enabled, the Importer checks if a user/people record with the same PIN Only credential exists in the SMS database. If one exists, the Importer will not create a new cardholder record. If this option is not enabled, the Importer will not try to match PIN Only records.
- **Also require name Match for RCD match** - If this option is enabled, the Importer not only matches the credential data, but also the last and first name. Enabling this option avoids the potential mix up described above with John Doe and Mary Jane, but poses a different problem; if someone is entered as "John Doe" in LockLink, but as "Jonathon Doe" in SMS, they will not be matched if this option is enabled.

- a) **Attempt to match existing Cardholders by Name** - Enabling this option forces Importer to match newly imported cardholder records with records already present in the database by name.

Before inserting a new cardholder (which are called "users/people" in LLE and LL7), the importer checks if any existing cardholder records have the exact same last and first name, and if so, imports that user's access, user groups, and credentials into the existing cardholder record. This is similar to the match by RCD option, except name rather than card number is used as the matching criteria. Operators should be careful, since misspelled names, and common names shared by several people (i.e. "John Smith") can cause erroneous import.

- b) **Prepend LL7 Building and LLE Facility Name** - If this option is enabled, the Importer prepends either the building name (LL7) or facility name (LLE) when importing new CM doors. This is useful in cases where there are multiple doors sharing the same name in LockLink. For instance, with this option turned on, if both "Building A" and "Building B" contain a door named "Room 123" in the source LockLink 7 database, they will be imported as "Building A - Room 123" and "Building B - Room 123" respectively. This is much clearer than the default behavior (with this option off), which creates two records called Room 123 with an automatically generated unique number at the end of each name in SMS.
- c) **PINS with leading zeros** (system does not allow leading zeros) - Importer now has selectable behavior to deal with leading zeroes.
- **Strip leading zeros** (Cardholders should be informed of changed PINs) - Unlike LockLink, SMS does not allow either "PIN Only" or "plus PIN" credentials to have a leading zero. Previous versions of the Importer, as well as the current version removes leading zeros when this option is selected. This can cause problems because the resulting number may be too short, or conflict with other numbers (for instance 012 would be changed to 12, which is too short for a pin, and 01234 would be changed to 1234, which could conflict with a pre-existing pin 1234.). In addition, it is problematic, because affected cardholders need to be informed that their PIN numbers have changed. In such cases, the following option can be used as an alternative method.
 - **Change leading zeros to nines** - Enabling this option replaces any leading zero digit with a nine. (So 012 would change to 912, and 001234 would change to 901234). Since, on CM locks with 6 button keypads, nine and zero share a single button, this can be done without affecting the day to day usage of cardholders. However for CM locks with 12 buttons keypads, cardholders should be notified of their new PINs.



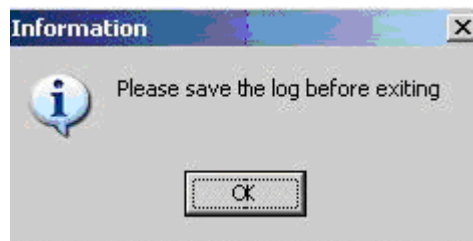
- 6 The import process starts and displays the **Performing Import** window. The application goes through several processes of reading the data; determining the Encoded IDs of the credentials, generating several sets of SQL scripts, and then applying these scripts. The progress bar display is updated several times from empty to full as these three processes are completed. The user may cancel this process by clicking the **Cancel** during this process.

Note: If the process is cancelled halfway through the applying scripts process, only half the data will be imported to the database. If the user chooses to cancel the process, it is highly recommended that the user restores a recent backup of the database afterwards.

- 7 Upon successful completion, the Finished window is displayed. Click **Finish** to exit.

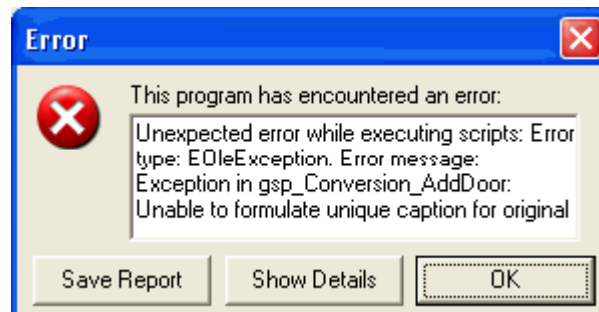
Warnings and Error Messages

Warnings indicate expected problems, such as records that were skipped because the technology is not supported by the Importer (Interflex or mechanical locks, RSI Handkey credentials, etc.). The user must save the log before exiting; until the log is saved, the **Finish** button is disabled. If the user attempt to exit without saving the log, the following message is displayed.

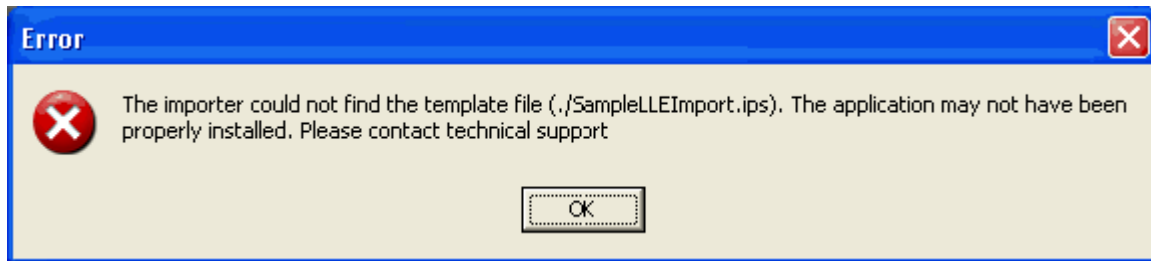


In addition, each item noted in the log is saved into the **Schlage SMS** database. This allows the information to be reported upon subsequently, even if the user discards this log.

If the Importer encounters unexpected conditions or an error, an error message like the one shown below is displayed. In this case, use the **Save Report** button to save the error log generated by the importer. Users can email these reports to techsupport_schlegesms@irco.com. The saved report must be attached with the message before sending. Savvy users may want to look at the details with the show details button to get an idea what might have gone wrong.



The following screen is displayed if the “SampleLL7Import.ips” file is missing as described earlier in this document.



Once the error message is dismissed, the user must exit the application.

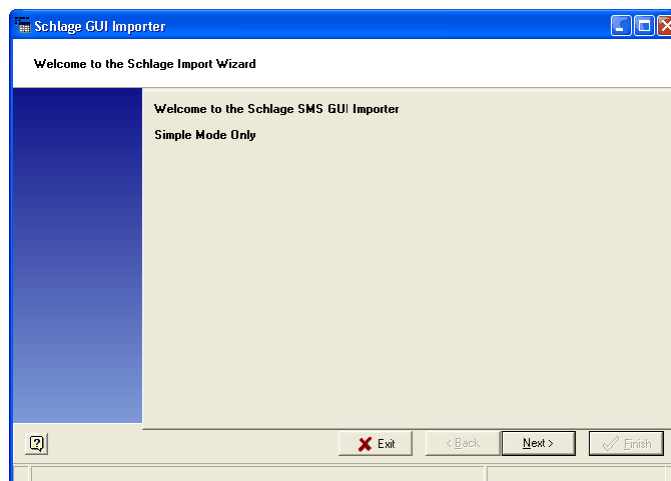
Schlage GUI Importer

CHAPTER 49

Introduction

Schlage GUI Importer allows users to import cardholder information from delimited text files. Using the Importer you can insert cardholder records along with their online/offline credentials. The user can also import an additional PIN only credential for each cardholder record.

Note: The GUI Importer does not attempt to handle the case where a total integration of the database to some external real-time source (such as an oracle HR database) is required. That type of integration requires data relationships that are not well represented by flat files such as csv or xls (such as the ability to selectively include or exclude cardholders from multiple groups using different timezone parameters). See **Schlage Advanced Importer** for a more complex and flexible importing framework designed to handle this case. To know more about this program contact IR technical support.



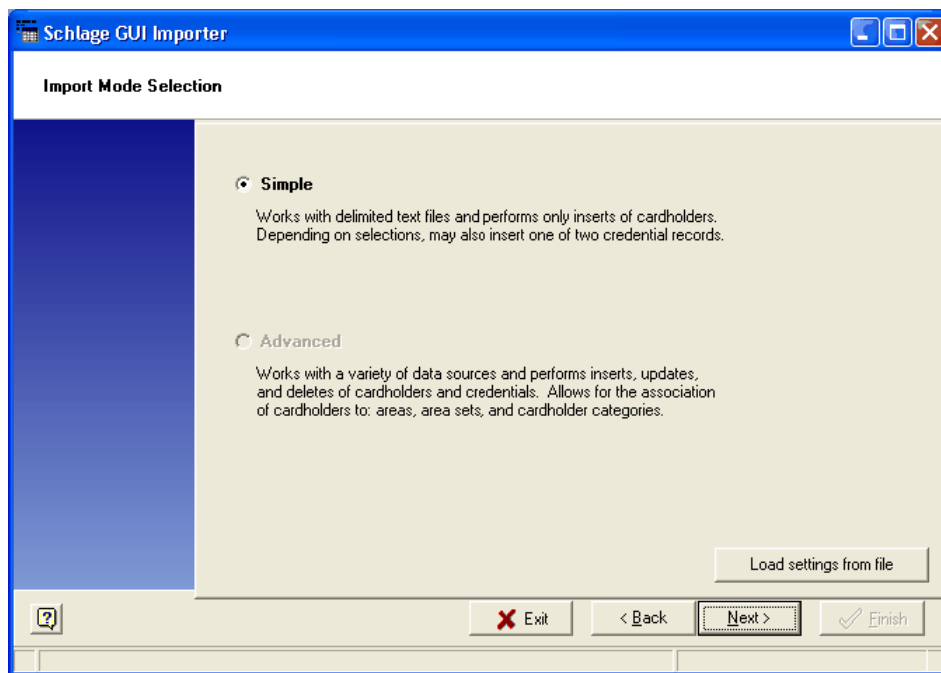
Working with GUI Importer

Overview

The current version of the Importer works only in the **Simple mode** which imports delimited text files. The import wizard leads you step by step through its screens for importing cardholder records from text files.

Importing text files

- 1 Open the **Schlage GUI Importer** program from the Bin directory.
- 2 The **Welcome** window opens. Click **Next**.
- 3 Next step is the **Import Mode Selection**. Since the program is currently available only in the **Simple** mode, it defaults to Simple mode, and the Advanced mode is disabled. If the settings (the import options and the mapping of columns) for the import are already saved to a file, you can load the settings from that file by clicking on the **Load settings from file** button located at the bottom of this window.



Import Options

- 1 Next step is selecting the options for import.

Schlage GUI Importer
Simple Import - Options

Import from File: C:\Documents and Settings\skrishna\My Documents\5.2\Names.txt
Delimiter Character: , (comma)
Quote Character: (none)

Header Lines To Skip: 1
☒ Use Header Line for Column Names? Header Line: 1

☒ **Delete Existing Cardholders Before Importing**

Error Behavior:
☒ Skip record and continue ☐ Halt import

Preview: Preview includes the top 25 of 100 rows ☐ Preview All Rows

Last Name	Initial	First Name	Pin Only	Plus PIN	EncodedID	RawCardData	Notes	Online2	Sp
Poulsen	N	Sarah	1111	1111	1	400000002	Notes: Special Access	1	xxx
Martins	E	Mia	1112	1112	2	400000004	Notes: Special Access	2	xxx
Couture	C	Aoife	1113	1113	3	400000007	Notes: Access to Development 3		xxx
Hämäläinen	N	Madison	1114	1114	4	400000010	Notes: Access to Development 4		xxx

Parsed 25 of 100 Rows

- a) First select the text file to import. Click on the browse button to locate the text file.
- b) Next, select the **Delimiter Character**. This character is required to separate the fields and create individual columns while importing the data. E.g. There must be a separator between First name and last name texts in order for the program to create separate columns for these two text fields in the system. You may either choose the delimiter character from the drop down menu (comma, pipe and tab are the options), or type in a custom character.
- c) Now select the **Quote Character**. You may choose quotes (" ") or type in your own quote character. Quotes allow to keep separated text in a single column. E.g. If the last name of a person is "Smith, Jr", the user must keep the two words in quotes to keep them in a single column.
- d) Select the number of lines (if any) to skip while importing data. If the text file contains a header line, you must specify the number of the line, so that line is not used as a cardholder record while importing. Also, if the text file has some comments in front of the data lines, you can ask the importer to skip those lines. The minimum number of lines to skip is zero (0).
- e) Select the option **Use Header Line for Column Names** to have specific headers for the imported data. The text in the header line specified in the next step is used as column names. See in the example above LastName, Initial etc are used as headers.
- f) Now specify the number of the line that you want the program to use as a header line. This step is available only if the Use Header Line for Column Names is selected.
- g) Selecting the option **Delete Existing Cardholders Before Importing** deletes all the existing cardholder records in the system, and loads the data in the imported file.
- h) The **Preview** section updates itself in real-time, and shows the content of the text file that is being imported. In the example above, we asked the program to skip the first line, and use the first line as the header. So the headers show as FirstName, Initial, LastName etc. If the text file does not contain a header, the program generates the header names as Field A, Field B and so on.

Linking source columns with Cardholder fields

In this section you may link the columns in the source file with the cardholder fields in the system.

Simple Import - Demographics

Last Name: A - Last Name | First Name: C - First Name | Initial: B - Initial | Notes: J - Notes

Choose which source column represents cardholder Notes.

Preview

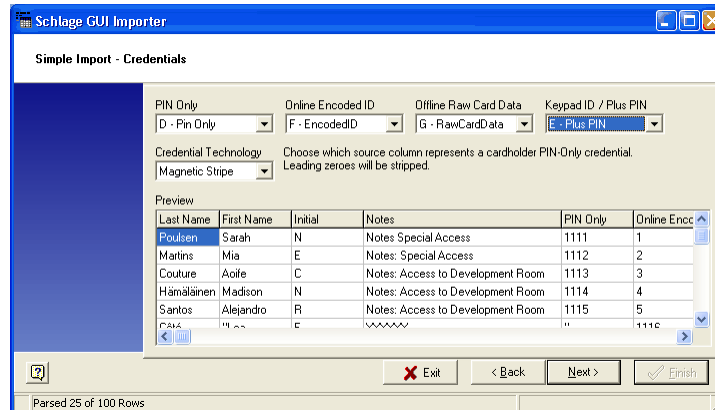
Last Name	First Name	Initial	Notes	PIN Only	Online Encoded ID	Offline
Poulsen	Sarah	N	Notes: Special Access	Do Not Import	Do Not Import	Do Not Import
Martins	Mia	E	Notes: Special Access	Do Not Import	Do Not Import	Do Not Import
Couture	Aoife	C	Notes: Access to Development Room	Do Not Import	Do Not Import	Do Not Import
Hämäläinen	Madison	N	Notes: Access to Development Room	Do Not Import	Do Not Import	Do Not Import
Santos	Alejandro	R	Notes: Access to Development Room	Do Not Import	Do Not Import	Do Not Import
Côté	Lea	F	Notes: Access to Training Room	Do Not Import	Do Not Import	Do Not Import
Wilson	Jesse	V	Notes: Access to Training Room	Do Not Import	Do Not Import	Do Not Import
Andersen	Anna, Jr.	E	Notes: Access to Training Room	Do Not Import	Do Not Import	Do Not Import
Mägi	Aleksi	S	Notes: Access to Development Room	Do Not Import	Do Not Import	Do Not Import
Lima	Ronald	M	Notes: Access to Training Room	Do Not Import	Do Not Import	Do Not Import
Kova?	Markus	J	Notes: Access to Development Room	Do Not Import	Do Not Import	Do Not Import

Parsed 25 of 100 Rows

- Last Name** - Using the drop down menu, select the column in the source file that contains last names of the cardholder. The source file we used for this example already has a header named LastName and that is column A. So the column that is linked here with Last Name field is A - LastName. Last name is a required field.
- First Name** - Like the previous field, choose the column that contain first names of the cardholders. This field defaults to "Do not Import" by default (optional field). This allows the user to skip this field from mapping.
- Initial** - Using the drop down menu, choose the column in the source file that represents the field Initial (optional field, defaults to "Do not Import").
- Notes** - Choose the column in the source file that represents this field. The choice by default is "Do not Import" (optional field).

Credential Import Choices

In Simple mode, the program allows to import one credential and an additional PIN only credential for cardholders. The following window allows you to specify these options. All the fields available in this step are optional, and defaults to "Do not Import" option.



- Pin Only** - Select the source column that represents this field. If this is selected, PIN Only credentials are inserted for the cardholders in the source file using the value in the linked field as the PIN value. Leading zeroes will be stripped. This field defaults to "Do Not Import" value.
- Online Encoded ID** - Select the source column that represents Online Encoded ID. If a valid source is selected, credential records are inserted for these cardholders. The value in the corresponding field in the source file is used as Encoded ID. Leading zeroes will be stripped. This field defaults to "Do Not Import" value.

In addition to the columns, a choice of "Derive from offline" is also available from the drop down menu. If this is selected, the system tries to generate Encoded ID from the raw data. This is a valid choice only if the raw data value is set to a valid source column, rather than "do not import". Also, both Encoded ID and Raw Data cannot be set simultaneously to "Derive from ..."

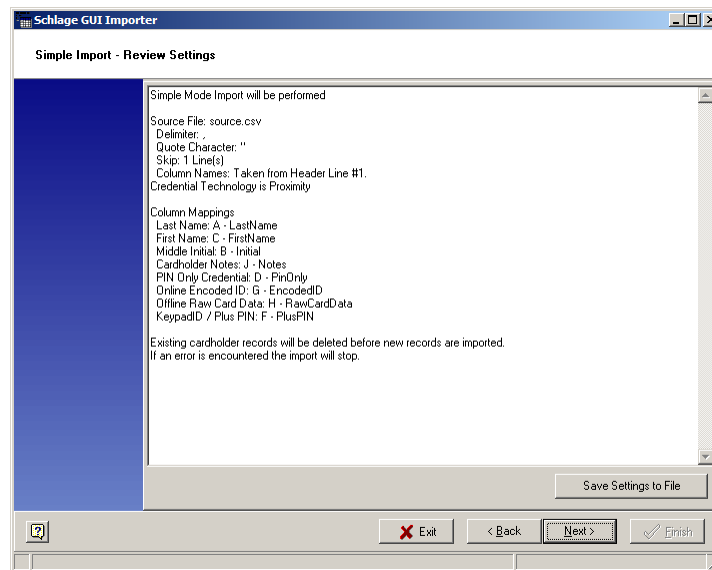
- Offline Raw Card Data** - Select a source column that represents raw card data. If a valid source is selected, credential records are inserted for cardholders, using the value in the corresponding source column. Leading zeroes will be stripped. In addition to the columns, a choice of "Derive from Online" is also available from the drop down menu. This field defaults to "Do Not Import" value.
- Keypad ID/Plus PIN** - Select a source column that represents this field. If the Encoded ID and Raw Card Data fields are set to "Do not Import", this field is disabled.
- Credential Technology** - Select a source field represents the credential technology that will be used when inserting these credentials. This field is set to "Magnetic Stripe" by default. PIN Only is not included in this list. This field is disabled if both Encoded ID and Raw Data are set to "Do not import".

If Offline Raw Card Data is selected, the credential technology must be one of ibutton, Magstripe, Proximity. It cannot be set to barcode or barium ferrite.

Note: The Encoded ID, RawCardData, and keypadID will be saved in the same credential record. The PIN Only credential is stored in a separate record.

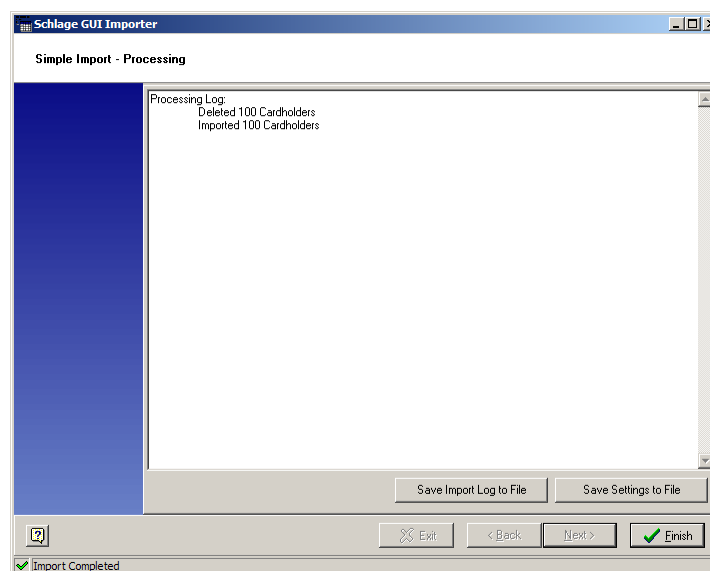
Review screen

The following window displays the selections you made in the last two steps. You can save these settings to a file by clicking the **Save Settings to File** button. The Load setting from file option in the Import Mode selection window allows users to later use this saved settings file. Click **Next** to begin the import process.



Log file

Once the import process is complete, the following window is displayed with the log of the actions it performed. You have options to **Save Import Log to File** and **Save the Settings to File**. Click **Finish** to exit the program.



Advanced Importer

CHAPTER 50

Introduction

The **Schlage Advanced Importer** allows users to import information from text files to the Schlage SMS database on a scheduled basis. The Importer has a command line parser that can be invoked either manually or via a scheduler to process the text files with specific command format.

Overview

The Importer allows only text files to be imported to Schlage SMS database. The information in the text file which is being imported must be in a specific format as outlined below; header lines and other errata contained in the file and some settings associated with the import that must be set in the database.

Text file format

Each line of data in the text file that is imported contains a "command". The structure of each line in the text file varies based on the type of command contained in the source file. Different commands are used to separate information like comments, header, version etc. These settings associated with the import must be set in the database prior to importing any data.

Comment lines

Any line in the file that begins with forward slashes, (//) is treated as a comment by the Importer. Spaces at the beginning of the line and partial line commenting (i.e. commenting anything after two slashes in the middle of the line) is not supported.

Example of a comment line:

```
// Registration (export) for Access Control System (import)
```

Headers

Valid import header consists of version number (version of the Schlage SMS) and look up value used to retrieve import settings. The program is shipped with default import settings, and the look up key for "Import_Default Settings" is provided. Keys are case sensitive. All look up keys should begin with "Import_". This will avoid conflict with other entries in the LMSettings table.

Example of a header:

Example header - minimal:

```
5.1.6.0
```

Import_DefaultSettings

Command lines

Each line subsequent to the header in the file contains a single import command and its associated parameters. The lines are broken up into a series of tokens separated by delimiters. The details of this are configurable by settings described later. The first token of each line contains the command identifier; subsequent tokens contain the parameters needed for that command. Parameter tokens can in some cases be left blank to use a default value; some tokens however cannot be left blank.

Example of a command line:

```
COMMAND_IDENTIFIER,parameter 1,,parameter 3
```

In all cases, having an invalid number of parameters on a line or otherwise malformed data will cause the parser to generate an error. A setting in the database determines if the parser should halt entirely or skip the offending line and continue.

Steps for running the Importer

Prerequisites

- 1 The database will be installed with the “Default Settings” for the importer. Default settings are loaded by the DL_ImportSystemDefaultSettings.sql script.

Note: Review the Import Settings section for more information on the file format, field delimiter etc.

- 2 Identify the operations that you want to perform with the data. For example; add cardholder, add credential or delete area access etc.
- 3 Identify the appropriate commands for these operations from the command reference section of the document.
- 4 Create a text file according to the field specifications in the **Default Settings** section. The recommended file format is comma delimited with no quotes. Note that if the file is comma delimited, then commas are not allowed within the values themselves. If commas are required in fields (such as a last name of Jones, Jr.), the use of a pipe delimited non quoted format is recommended.
- 5 Create one line per command.
- 6 Create commands in the proper sequence.

For example; if you are adding a new cardholder, assigning a credential, and granting new cardholder access to an area and area set, the commands are:

```
ADD_CARDHOLDER  
ADD_CREDENTIAL  
ADD_AREA_ACCESS  
ADD_CARDHOLDER_AREA_SET_LINK
```

If you are deleting or modifying the cardholder access, the commands are:

```
DELETE_AREA_ACCESS  
DELETE_CARDHOLDER_AREA_SET_LINK
```

- 7 Make sure that each command is followed by the appropriate number of parameters.

For example: ADD_CREDENTIAL requires 11 parameters.

- 8 Make sure that the parameters appear in the right order
- 9 The last line of the file may be END_OF_FILE.

Manual execution

- 1 After creating the file, run the parser from the command line by doing the following steps:
- 2 Go to the command prompt
- 3 Go to the directory where the parser executable is stored
- 4 Run the parser program by entering the following command:

usage: import -I inputfile (required)

[-S server] (default = local)

[-D use database name] (default = SchlageSQL)

[-E] trusted connection

or

[-U login id]

[-P password] (applies to database authentication)

[-F] END_OF_FILE command required

[-B] display Begin and end date & time stamps

[-T] display Transact-SQL

[-A] Audit only - do not execute Transact-SQL

[-W] skip waking the System Processor (SP)

[-? show this syntax summary

Example: SMSImportParser.exe -E -SSQLone -IDataFile.TXT

The above example will attempt to import the file DataFile.TXT, using a trusted connection to the SQL server named SQLone

Scheduling for Automatic Import

You can use the NT scheduler to run the Importer

Import Settings

The program is shipped with default settings. These settings are stored in the LMSettings table of SchlageSQL. The database will be installed with all values filled in for the default lookup key of "Import_Default Settings".

The recommended file format is comma delimited with no quotes. Note that if the file is comma delimited, then commas are not allowed within the values themselves. If commas are required in fields (such as a last name of Jones, Jr.), then use a pipe delimiter.

The values in parenthesis following each setting indicate what the value will be for Default_ImportSettings.

- 1 Delimiter(,) - This must be set to a single character. Typically, a comma or a vertical pipe symbol (|). Unless the values are quoted, the delimiter is not allowed as part of the value and this will result in an error.
- 2 UsesQuotes (0) - This must be set to 0 or 1. This determines if the values in the string are quoted.
- 3 QuoteCharacter (") - The character is used to quote values in the text file. This is ignored if UsesQuotes is false. This character must be different than the delimiter character. If quotes are used, quote characters are not allowed within the value, and this causes an error. Escape sequences are not supported.
- 4 UDFDelimiter (=) - The character used to separate FieldName=Value pairing that are specified as parameters in UPDATE_USER_DEFINED_FIELDS command. This must be set to a single character. Typically = (equal sign) or : (colon).
- 5 CardholderUniqueIDFieldName (CardholderID) - Specifies which field is being used as the unique cross-referencing field for cardholders. This is typically a User Defined Field, although it could also be CardholderID. The field should be an integer or string. Typically users will create a string UDF such as StudentID or EmployeeID or SocialSecurityNumber and use this field.
- 6 HaltOnInvalidData (1) - This must be set to 0 or 1. When this is 0, lines that are malformed (i.e. too many parameters, too few, invalid command indicator, etc) or invalid (i.e. ID number or caption is not found in database, etc) are skipped and logged as an error, but the rest of the file will still be processed. When this is 1, the process halts entirely after logging an error message when it encounters invalid data.
- 7 ProcessAmbiguousMatches (ProcessAmbiguousMatches (0) - This affects the ADD_CARDHOLDER and UPDATE_CARDHOLDER commands and must be set to 0 or 1. When this is set to 0, any "add" line whose UniqueID already exists in the database will be not be processed and an error will be logged in the Exception Table. Likewise, any update whose UniqueID does not exist in the database will be logged. If HaltOnInvalidData is set to true, such a case will also cause the process to halt regardless of this setting.

When this is set to 1, any "add" row whose UniqueID already exists in the database will be treated like an update and any update whose UniqueID does not exist in the database will be treated as an add. These rows will be logged in the exception table as well, but the process will not halt or skip processing of the row and data will be updated or inserted.

- 8 DefaultActivation (1970-01-01 00:00:00) - Used for both Cardholder and Area Access records. Specify a Default Activation date for cardholder activation using yyyy-mm-dd format or a "relative to now" date by using a signed integer value.

Default Activation setting	Activation date
2006-08-25	August 25, 2006
+2	2 days from moment of import
+0	moment of import
-14	2 weeks prior to the moment of import

- 9 DefaultExpiration (2038-01-01 00:00:00) - Used for both Cardholder and Area Access records. Similar to Default Activation, the value of the setting may be a proper date or a "relative to now" signed integer value.
- 10 DefaultAPControlled (1) - This setting is used for setting antipassback. This must be 0 or 1.

- 11 DefaultBlocked (0) - This must be 0 or 1 and is used for both Cardholder and Area Access records.
- 12 DefaultPersonWithDisability (0) - This must be 0 or 1.
- 13 DefaultAreaPrivilege (1) - This may be any valid integer, but only the lowest order 8 bits are considered.
- 14 DefaultDoorPrivilege - This may be any valid integer, but only the lowest order 8 bits are considered.
- 15 DefaultTimezoneID (1) - This must be the TimezoneID of a valid Timezone defined in the system. 1 indicates the "Always" Timezone.
- 16 DefaultBadgeLayoutID (0) - This must be the Badge Layout ID of a valid badge layout defined in the system. Any value equal to or less than zero will be treated as null, meaning no badge layout will be associated with a credential when it is added.
- 17 DefaultBadgeTechnologyID (0) - This represents a Badge Technology record within the Badge Technology table.
Supported values are:
 - a) (Barium Ferrite)
 - b) (Magnetic Stripe)
 - c) (Proximity)
 - d) (PIN Only)
 - e) (iButton)
- 18 DefaultCardformatID (0) - This must be the Card FormatID of a valid card format defined in the system. Any value equal to or less than zero will be treated as null, meaning no card format will be associated with a credential when it is added.
- 19 DefaultCredentialFunctionID (0) - This must be an integer between 0 and 11 (inclusive).
- 20 DefaultCredentialRetirementStatus (0) - This must be the Badge StatusID of a row in the Badge Status table. 0 indicates Cardholder Deleted. It is assumed by the RETIRE_CREDENTIAL and RETIRE_ALL_CREDENTIALS commands if no value is specified for the Badge Status parameter.
- 21 DefaultSiteCode e(0) - This must be an integer value. Any value equal to or less than zero will be treated as null, meaning no card format will be associated with a credential when it is added.
- 22 DefaultIssueCode (0) - This must be an integer value. Typically this is 0 or 1, since some systems begin a card with issue code 0, while others begin with issue code 1.

Supported commands

The following is the list of commands that are used in the text file to import cardholder data into Schlage SMS database.

Commands for adding and deleting cardholders

Supported Commands

The following is the supported commands for adding and deleting cardholders and their parameters.

- 1 **ADD_CARDHOLDER** - This command creates a new cardholder in the system. Given below are the parameters used with Add Cardholder command.

- a) **UniqueID** - Unique ID is an identifier used to uniquely match a cardholder record. In general this will be a User Defined Field which has been populated from an external system, although it could also be the CardholderID field. What exact field this refers to is stored in the import settings. This may be an integer or string. This value must not be left blank. If the unique identifier is CardholderID, the value supplied is ignored, as the CardholderID is automatically generated by Schlage SMS.

This is the line in the import settings that determines the unique ID.

```
EXEC gsp_InsertLMSetting NULL , NULL, @WksID, @Section, N'CardholderUniqueIDFieldName',  
@stString, N'CardholderID'
```

- b) **Activation (date & time)** - This is the date and time that indicates the time at which the cardholder's access privileges become valid. It may be left blank to use the settings default activation time. In determining whether a particular access record has become active yet, the system will use the default cardholder activation date and the area access activation date.

The officially supported format for the date and time is yyyy-MM-dd HH:mm:ss, such as: 2006-05-31 23:59:59

- c) **Expiration (date & time)** - This is a datetime that indicates the time at which the cardholder's accesses expire and are no longer valid. It may be left blank to use the settings default. In determining whether a particular access record has expired yet, the system will use the earlier of the cardholder expiration date and the area access expiration date.
- d) **APControlled (boolean)** - This determines if the cardholder is subject to anti-passback rules. This may be left blank to use the settings default.
- e) **LastName** - This is a string field that must not be left blank.
- f) **Firstname** - This is a string field. If left blank, the cardholder will simply have a blank first name.
- g) **Initial** - This is a string field. If left blank, the cardholder will simply have a blank middle initial.
- h) **Blocked (boolean)** - When set to true (1), all access for this person will be denied. This may be left blank for a default.
- i) **Description** - This is an optional string field. It may be used to hold any notes about the cardholder. It has no particular value related to access beyond a place to store notes. If left blank, the cardholder will simply have a blank description.
- j) **PersonWithDisability (boolean)** - When set to true, "Valid Access, Special Access Privilege" transactions will be generated at readers instead of normal "Valid Access" transactions for the cardholder in question. These special transactions may be used to trigger a different set of events (for instance, opening a door for a longer period of time, or opening a gate instead of a door) to assist the cardholder with entry. This field is irrelevant to offline locks.
- 2 UPDATE_CARDHOLDER** - This command has the exact same parameters as ADD_CARDHOLDER. However, the behavior of default values is a bit different than the add command. Anything left blank that would have resulted in a default value (i.e. activation, expiration, APControlled, etc.) will instead retain the existing value of the field for that record. Fields left blank without a default (i.e. Description) will be set to blank. Required fields (i.e. UniqueID) must not be left blank.
- 3 DELETE_CARDHOLDER** - This command will delete the cardholder record identified by the UniqueID. All associated badges are retired and associated access is deleted.

Commands for adding, retiring, and deleting credentials

- 1 ADD_CREDENTIAL** - This command will add a credential to the system for the cardholder identified by the unique ID.
- a) **StampedID (integer)** - This field represents the hot stamp number physically displayed on many credentials. This may be left blank for credentials that do not have a stamped id (resulting in a null value being stored).

- b) EncodedID - This is an identifier that is both unique to the credential and physically encoded on the credential. Although declared as a string type to support a few rare types of credentials, this is almost always a numeric value and is treated as such by the import system. The maximum numeric value for encoded id is 4294967295 (the most an unsigned integer will hold)2147483647. If an EncodedID that is larger than this or less than 1 is supplied, it will cause an error. Leading zeroes are truncated. All credentials must have an encoded id that is unique among active (but not among retired) credentials.

In Magstripe cards for instance, this is usually a student or employee id number encoded on a portion of track 2. (Other portions of track 2 may include extra data, such as site code or issue code, that are not part of the encoded id). All credentials must have a encoded id that is unique among active (not retired) credentials.

- c) IssueCode (integer) - This represents a value that is incremented each time a cardholder loses a credential and is reissued a credential with an identical encoded id. This may be left blank for credentials that do not have an issue code encoded on them (resulting in a null value being stored).
- d) BadgeLayoutID - When badge printing is utilized, this identifies which print layout should be used when printing this credential. It may be left blank (resulting in a null value being stored).
- e) BadgeTechnologyID - This indicates the type of credential and may be left blank to use a default value. Supported values are:
 - (Barium Ferrite)
 - (Magnetic Stripe)
 - (Proximity)
 - (PIN Only)
 - (iButton)
- f) KeypadID - If a pin number PIN must be entered along with presentation of the credential, that a pin number must be stored here. TODO – determine the maximum length of a PIN number. Talk about leading zeroes. Talk about default value or lack thereof
- g) CredentialFunctionID - This indicates the function of the credential at an offline lock and may be left blank to use a default value. Online locks do not support credential functions. Supported values are:
 - 0 (Normal)
 - (Super User (Pass Through))
 - (One time/Visitor)
 - (Supervised)
 - (Toggle)
 - (Lockout)
 - (Dogging)
 - (Prohibit)
 - (CT - Aux Normal)
 - (CT - Main Aux Normal)
 - (CT - Aux Toggle)
 - (CT - Main Aux Toggle)

- h) **RawCardData** - This field should contain all the data encoded on the credential and is required for clients using CM locks or CT controllers. These offline locks do not parse credential data into separate fields such as encoded id and site code. Instead they look at all of the data on the credential after subjecting it to a bitmask. While in some cases it is possible to use a subset of the full credential data for this field, this is not recommended as subsequent changes to the badging scheme may require re-enrollment of all users. It is always preferable to have all of the credential data stored in the database. For Magstripe credentials, this does not include the start and stop sentinels or LRC character. RawCardData is not evaluated by online controllers.
 - i) **CardFormatID** - Card formats store information about the layout of data on the credentials and are useful in many installations, especially wherever multiple card formats are used or when both online and offline locks are used simultaneously. This field may be used to identify which card format a credential has been encoded with. This may be left blank (resulting in a null value being stored).
 - j) **SiteCode** - This may be left blank for credentials that do not have a site code (resulting in a null value being stored).
- 2 RETIRE_CREDENTIAL** - This will retire a single credential matching the encodedID EncodedID for the cardholder.
- a) **UniqueID** (nvarchar or integer)
 - b) **EncodedID** (nvarchar(16))
 - c) **StatusID**(integer)
- This must be the BadgeStatusID of a row in the BadgeStatus table. 0 indicates Cardholder Deleted. If no value is specified then the Setting DefaultCredentialRetirementStatus is assumed.
- 3 RETIRE_ALL_CREDENTIALS** - This will retire all credentials for the cardholder in question.
- a) **UniqueID** (nvarchar or integer)
 - b) **StatusID**(integer)
- This must be the BadgeStatusID of a row in the BadgeStatus table. 0 indicates Cardholder Deleted. If no value is specified then the Setting DefaultCredentialRetirementStatus is assumed.

Area Access Commands

The following are the Commands that affect area access

When considering these commands, it is important to note that a single specific cardholder may have more than one area access record for a single specific area. Each access record may have different time zones, expiration, etc. In addition, the linking of a cardholder to an area set will result in additional area access records being created; subsequently adding or removing areas to or from that set will also cause area access records to be added or deleted for that cardholder.

- 1 ADD_AREA_ACCESS_BY_CAPTION** - This will cause an area access record to be created for the specified cardholder at the specified area.
- a) **UniqueID** (nvarchar or integer) - This the identification number of the cardholder.
 - b) **AreaCaption** (nvarchar(64)) - Attempt to find a unique matching area based on this caption. If not found, or not unique, an error is logged, and the process will either skip this line or halt entirely.
 - c) **Activation** (datetime) - This is the date and time at which this particular access record becomes valid. It may be left blank to use the settings default. In determining whether a particular access record has become active yet, the system will use the later of the cardholder activation date and the area access activation date. Individual area access activation times are not supported by offline locks; in this case the cardholder activation time is always used. This may be left blank for a default.

- d) Expiration (datetime) - This is the date and time at which this particular access record expires and is no longer valid. It may be left blank to use the settings default. In determining whether a particular access record has expired yet, the system will use the earlier of the cardholder expiration date and the area access expiration date. Individual area access expiration times are not supported by offline locks; in this case the cardholder expiration time is always used. This may be left blank for a default.
- e) Blocked (Boolean) - When set to true, this access record will not be sent to the controllers and offline locks. This may be left blank for a default.
- f) AreaPrivilege (integer) - Areas are always in some kind of state – usually “normal” but possibly states such as “lockdown”, “strike”, or “emergency”. This field is a bitmap determining during which states access should be granted due to this record. This may be left blank for a default. Most installations simply use a value of 1 (indicating “normal”) in all cases. This field is not typically used beyond the default. This field is irrelevant to offline locks. This may be left blank for a default.
- g) DoorPrivilege (integer) - Every reader has a type – usually “pedestrian” but sometimes types such as “handicapped” or “vehicular access”. This field is a bitmap determining during which states access should be granted due to this record. This may be left blank for a default. Most installations simply use a value of 1 (indicating “pedestrian”) in all cases. This field is not typically used beyond the default. This field is irrelevant to offline locks. This may be left blank for a default.
- h) TimezoneCaptionID (integernvarchar64) - This field indicates which time zone should be used for this access. The import will attempt to find a unique matching tTimezone based on this caption; if not found, or not unique, an error is logged, and the process will either skip this line or halt entirely. It may be left blank for a default, specified in the “DefaultTimezone” setting.

The software installs with predefined Ttimezones of “Always” and “Never”. “Always” may be used as a valid caption here; “Never” however may not be used as a tTimezone to assign access. Attempting to use “Never: while assigning access will cause an error in the import process for this row. Also note that these predefined time zone captions can be changed in the GUI by users, and if so these captions will no longer be valid for the import. (The actual meaning of these two predefined zones cannot be changed in the GUI – just the caption used to label them).

A value of 1 will indicate “always”.

- 2 ADD_AREA_ACCESS_BY_ID** - This procedure is exactly the same as **ADD_AREA_ACCESS_BY_CAPTION**, except that the unique AreaID assigned by the Schlage system is used to identify the area, rather than the textual caption of the area.

- a) UniqueID (nvarchar or integer)
- b) AreaID (integer) - The AreaID (generated by Schlage when the area is created) used to identify the area. If the id is invalid (does not exist, previously deleted, etc.) an error is logged, and the process will either skip this line or halt entirely.
- c) Activation (datetime)
- d) Expiration (datetime)
- e) Blocked (boolean)
- f) AreaPrivilege (integer)
- g) DoorPrivilege (integer)
- h) TimezoneCaption (nvarchar(64))

- 3 DELETE_AREA_ACCESS_BY_CAPTION** - This command will cause all access records for a given area to be deleted for the specified cardholder. In the simplest case, only the cardholder UniqueID and the AreaCaption are supplied; in this case all access records for that area are deleted for that cardholder. If more parameters are supplied, the import will attempt to match on those fields as well; for instance, if the time zone of "Always" is supplied, any accesses he has at that area for the "Always" time zone are deleted but any accesses he has at that area for the "9-5 Mon-Fri" time zone will not be deleted. Also note that the area access records are deleted regardless of source - It is important to note that all area access records for the area and person in question are deleted; if one person has a direct access record to an area, as well as other multiple accesses records to the same area a single area (for instance with different time zones, or as a result of several his links to an area set links), all of these area access records will be deleted. If more specific behavior is required, the DELETE_AREA_ACCESS_BY_ID command should be used.
- a) UniqueID (nvarchar or integer) - This parameter uniquely identifies the cardholder and must be supplied.
 - b) AreaCaption (nvarchar(64)) - Attempt to find a unique matching area based on this caption. If not found, or not unique, an error is logged and the line is skipped. This parameter must be supplied.
 - c) Activation (datetime) - This parameter may be left blank,blank; in which case it is not considered when determining what area accesses should be deleted.
 - d) Expiration (datetime) - This parameter may be left blank,blank; in which case it is not considered when determining what area accesses should be deleted.
 - e) AreaPrivilege (integer) - This parameter may be left blank,blank; in which case it is not considered when determining what area accesses should be deleted.
 - f) DoorPrivilege (integer) - This parameter may be left blank,blank; in which case it is not considered when determining what area accesses should be deleted.
 - g) TimezoneCaption (nvarchar(64)) - This parameter may be left blank,blank; in which case it is not considered when determining what area accesses should be deleted.
- 4 DELETE_AREA_ACCESS_BY_ID** - This command will cause one specific area access record to be deleted.
- a) AreaAccessID (integer) - The AreaAccessID uniquely identifies an access record and is generated by Schlage when the access record is created.
- 5 ADD_CARDHOLDER_AREA_SET_LINK_BY_CAPTION** - This command will establish a link between the cardholder and the area set, thus granting access to all the areas in the set. In addition, subsequent addition or removal of areas from the set will add or delete appropriate area access records for this cardholder. The parameters passed to this procedure are analogous to those passed to ADD_AREA_ACCESS_BY_CAPTION.
- a) UniqueID (nvarchar or integer)
 - b) AreaSetCaption (nvarchar(64))
 - c) Activation
 - d) Expiration
 - e) Blocked
 - f) AreaPrivilege
 - g) DoorPrivilege
 - h) TimezoneCaption (nvarchar(64))
- 6 TimezoneIDADD_CARDHOLDER_AREA_SET_LINK_BY_ID** - This command will establish a link between the cardholder and the area set, thus granting access to all the areas in the set. In addition, subsequent addition or removal of areas from the set will add or delete appropriate area access records for this cardholder. The parameters passed to this procedure are analogous to those passed to ADD_AREA_ACCESS_BY_ID.
- a) UniqueID (nvarchar or integer)

- b) AreaSetID (integer)
- c) Activation
- d) Expiration
- e) Blocked
- f) AreaPrivilege
- g) DoorPrivilege
- h) TimezoneCaption (nvarchar(64))

- 7 DELETE_CARDHOLDER_AREA_SET_LINK_BY_CAPTION** - This command is similar to the DELETE_AREA_ACCESS_BY_CAPTION. The UniqueID and AreaSetCaption parameters must be supplied; other parameters are optional and used to specifically identify a subset of links when many links exists (with different time zones or expiration for instance). All matching links, as well as access records that exists as a result of these links, are deleted.

This command will cause all links between a specific person and area set to be deleted. It is important to note that all links are deleted; if one person has multiple links to the same area set (for instance, with different timezones), each is removed (and the area access records depending on these links).

Area access records that are not dependant on these links are not affected. For instance, if John Doe has 9am-5pm access to the "Broom Closet" by virtue of a link to the "Maintenance Area Set", and also has a 24/7 access to the "Broom Closet" that was created for him directly, only the former access is removed when the link to "Maintenance Area Set" is deleted.

- a) UniqueID (nvarchar or integer) - This parameter uniquely identifies the cardholder and must be supplied.
 - b) AreaSetCaption (nvarchar(64)) - Attempt to find a unique matching area set based on this caption. If not found, or not unique, an error is logged and the line is skipped. This parameter must be supplied.
 - c) Activation (datetime) - This parameter may be left blank, in which case it is not considered when determining what area set links should be deleted.
 - d) Expiration (datetime) - This parameter may be left blank, in which case it is not considered when determining what area set links should be deleted.
 - e) AreaPrivilege (integer) - This parameter may be left blank, in which case it is not considered when determining what area set links should be deleted.
 - f) DoorPrivilege (integer) - This parameter may be left blank, in which case it is not considered when determining what area set links should be deleted.
 - g) TimezoneCaption (nvarchar(64)) - This parameter may be left blank, in which case it is not considered when determining what area set links should be deleted.
 - h) UniqueID (nvarchar or integer) - AreaSetCaption (nvarchar(64))
- 8 DELETE_CARDHOLDER_AREA_SET_LINK_BY_IDCAPTION** - This command will remove a specific link by id. All area access records dependant on this link are removed as well.
- a) CardholderAreaSetLinkID (integer)
- 9 DELETE_ALL_ACCESS_FOR_CARDHOLDER** - This command will remove all access for the specified cardholder, along with any links to area sets or cardholder categories. It is useful if the intent is to subsequently rebuild a cardholder's access from scratch or to completely lock a cardholder out of the system.
- a) UniqueID (nvarchar or integer)
- 10 UPDATE_USER_DEFINED_FIELDS** - This command is used to update values in the User Defined Fields table. It is a somewhat unusual command in that the number of parameters is not fixed. Instead, Name and Value pairs are supplied because the UDF layout varies from one installation to another (which renders a fixed set of parameters useless).

- a) UniqueID (nvarchar or integer)
- b) NVPairing - Name/Value Pairing. In the format of UDFColName=UDFColValue, an equal sign being the default delimiter. If the import file is using quote chars, those quote chars are applied to the pairing as a unit. The name and value fields are not individually quoted:

Correct: "UDFColName=UDFColValue"

Incorrect: "UDFColName"="UDFColValue"

The character used to delimit Name and Value is an equal sign "=" by default and is stored in the Import Setting UDFDelimiter. Note that the field name itself may not contain the UDFDelimiter character, whitespace, the import delimiter or quote character, or any other characters prohibited in the name of a column in SQL Server.

Additional (optional) NVPairing(s)

Additional NVPairings may be appended to the end of the command, allowing for multiple User Defined Fields to be updated for specified UniqueID

Example:

```
"UPDATE_USER_DEFINED_FIELDS","98765","DepartmentName=Auditing"
```

Example:

The single command (directly below) is equivalent to the three that appear below it:

```
"UPDATE_USER_DEFINED_FIELDS","98765","DeptName=Auditing","MetalDetector=0","ParkingSpace=GRN192"
```

```
"UPDATE_USER_DEFINED_FIELDS","98765","DeprName=Auditing"
```

```
"UPDATE_USER_DEFINED_FIELDS","98765","MetalDetector=0"
```

```
"UPDATE_USER_DEFINED_FIELDS","98765","ParkingSpace=GRN192"
```

```
END_OF_FILE
```

This special command (made mandatory by the import parser's -F command line argument) may appear only as the final command of an import file. It serves as a marker to prevent premature processing of the import file while it is still being transferred. This command takes a single optional parameter, the count of the preceding commands in the import file.

- c) NonEOFCmdCount (integer) - This parameter specifies the number of commands (not counting headers, comments, blank lines or the END_OF_FILE command itself) that the import file contains. If no value is specified, then no count is made and no comparison is performed.
- 11 UPDATE_USER_DEFINED_FIELDS** - This is a somewhat unusual command in that the number of parameters is not fixed. Instead, FieldName=Value pairs are supplied because the UDF layout varies from one installation to another (which renders a fixed set of parameters useless).

The first instance of the equal sign character in a parameter determines the field name and value. Anything before the equal sign is treated as the field name and anything after the equal sign is treated as the value to be used to update that field. Note that the field name itself may not contain the equal sign, whitespace, the import delimiter or quote character, or any other characters prohibited in the name of a column in SQL Server.

Some examples of this command are:

```
UPDATE_USER_DEFINED_FIELDS,Nickname=Skip
```

```
UPDATE_USER_DEFINED_FIELDS|Age=42| FavoriteColor=Lime Green
```

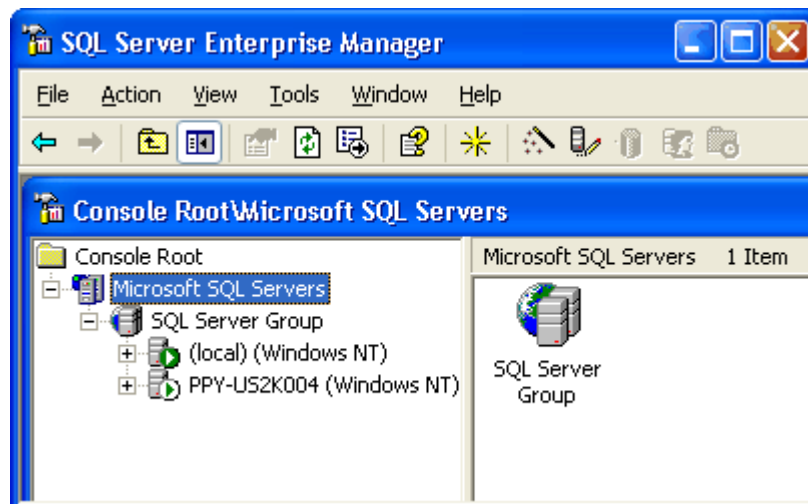
```
UPDATE_USER_DEFINED_FIELDS,"SupervisorsFullName=Doe, John","Title=Executive Assistant"
```

Appendix A: MSSQL 2000 Backup and Restore Procedures

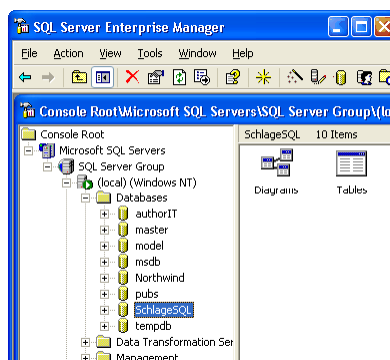
This section describes the procedures to be followed for backing up and restoring databases.

Backup SQL Database

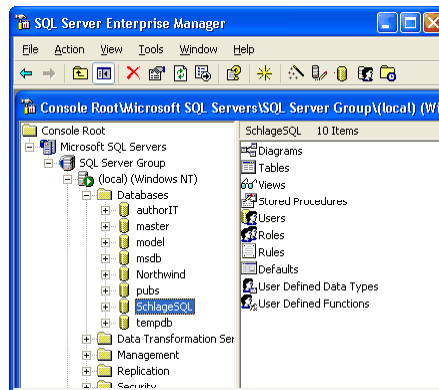
- 1 Go to **Start\Programs\Microsoft SQL Server\ Enterprise Manager**.
- 2 Left click the + icon for Microsoft SQL Server to expand the tree.
- 3 Once the green arrow appears, click the + icon.



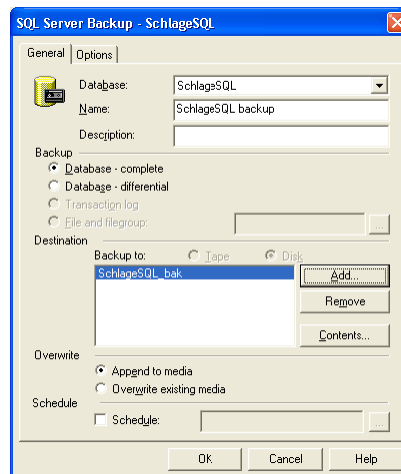
- 4 More folders are expanded. Click the plus icon next to the Databases folder.



- 5 Highlight the SchlageSQL folder to load the database information. You will see the right hand side of the pane load various SchlageSQL items.



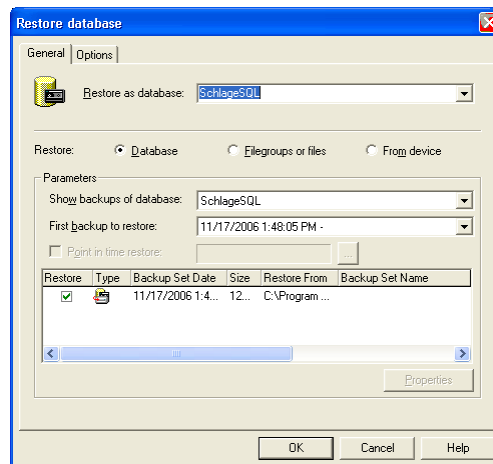
- 6 From the Tools menu, select "Backup Database".



- 7 The SQL backup window opens. Select the General tab.
- 8 In the Database field use the Browse button to select SchlageSQL.
- 9 In the "Name" field type SchlageSQL backup.
- 10 Next use the Add button to select the backup destination. SQL will default to the MSSQL Backup folder. Otherwise, you may browse to a folder of your choice.
- 11 In the File Name field of the Device Location window, type an easily identifiable name. The example shows, v515_SQL2K_AccessControlSystem.
- 12 Click the **OK** button.
- 13 Now select the Options tab. On this tab you want to check the **Verify Backup upon Completion** option. Click **OK** and the backup job will start and verify
- 14 Once the backup has completed successfully, click the **OK** button.

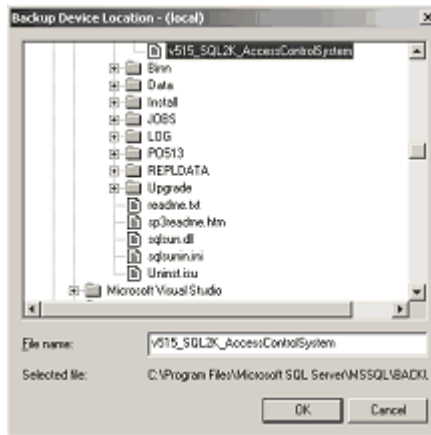
Restore SQL Database

- 1 In **Enterprise Manager**, left click the + icon for **Microsoft SQL Server** to expand the tree.
- 2 Once the green arrow appears, click the + icon.
- 3 More folders are expanded. Click the plus icon next to the Databases folder.
- 4 Highlight the SchlageSQL folder to load the database information. You will see the right hand side of the pane load various SchlageSQL items.
- 5 From the Tools menu. Select the “Restore Database” menu item.
- 6 On the General tab, select SchlageSQL in the Restore database field.
- 7 Next, click the “From Device” radio button.
- 8 Choose “Database – complete” in the “Restore backup set” field.

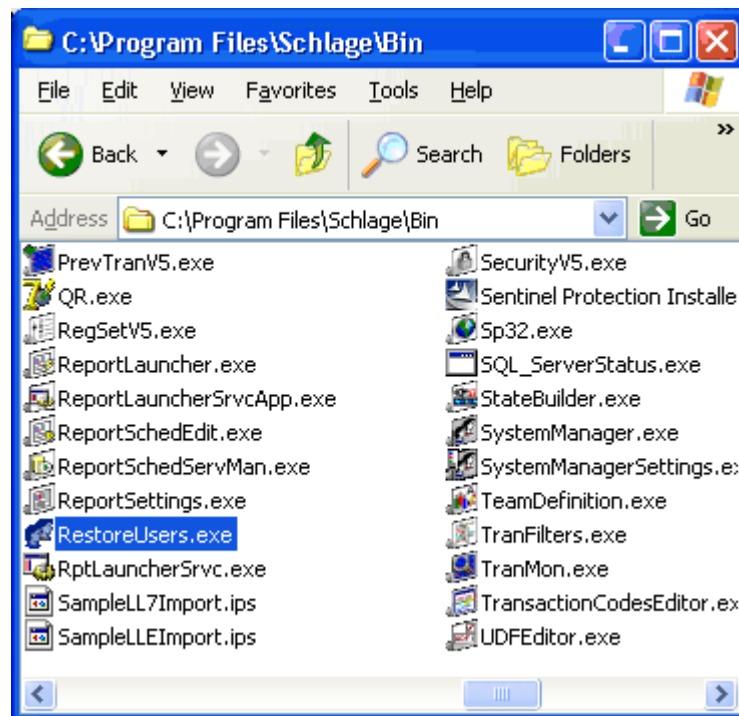


- 9 Click the **Select Devices** button to open the Restore Devices window.
- 10 Use the Add button to open the Restore Destination window.
- 11 In the “File Name” field, use the **Browse** button to locate the file to be restored.

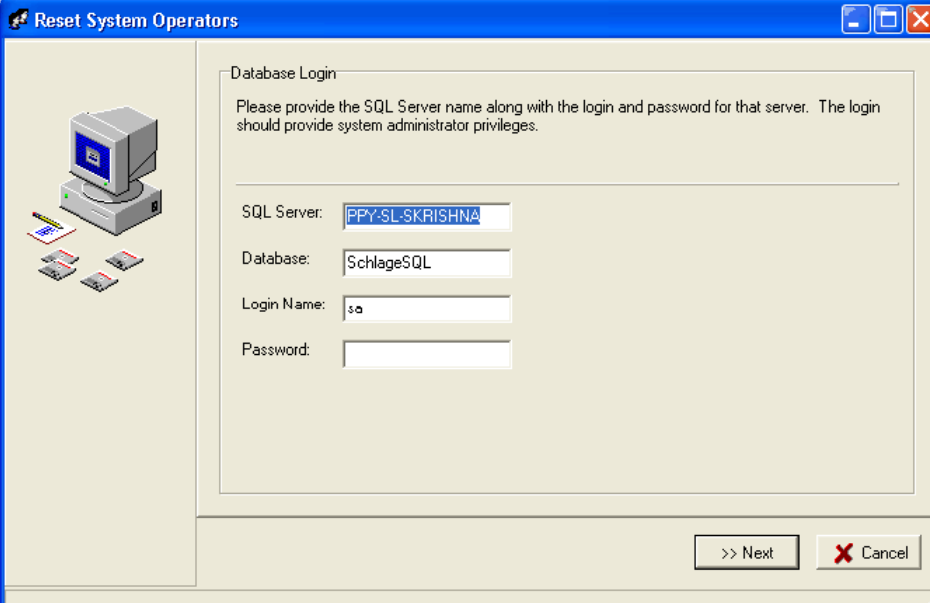
- 12 Highlight the file in the Backup Device Location window. Be sure to verify that it appears in the File Name field.



- 13 Click **OK** on all windows to begin the **Restore** procedure.
- 14 Once the restore has completed successfully, click **OK** to return to the main window of Enterprise Manager.
- 15 Under the \\Schlage\Bin folder, double click RestoreUsers.exe to open the application.

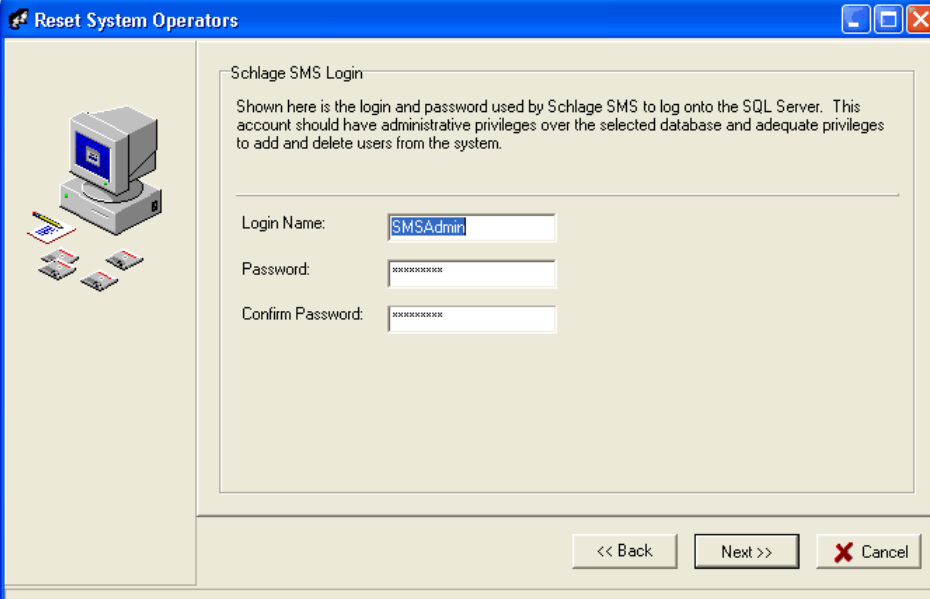


- 16 Enter the password for the database login and click Next.



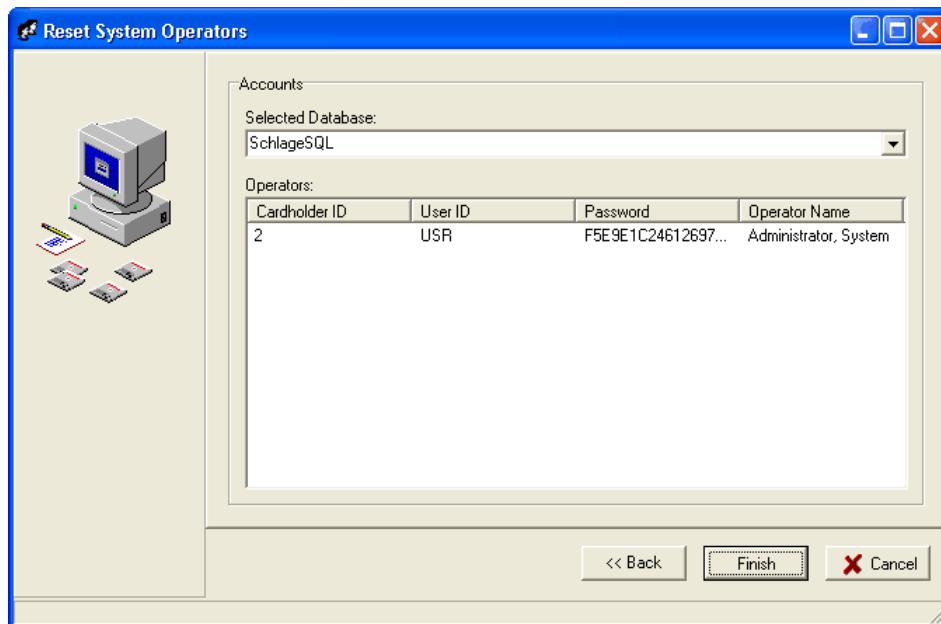
The 'Reset System Operators' dialog box is shown. It has a blue title bar and a light beige background. On the left, there is an icon of a computer with a monitor and keyboard. The main area is titled 'Database Login' and contains the following text: 'Please provide the SQL Server name along with the login and password for that server. The login should provide system administrator privileges.' Below this text are four input fields: 'SQL Server:' with the value 'PPY-SL-SKRISHNA', 'Database:' with the value 'SchlageSQL', 'Login Name:' with the value 'sa', and 'Password:' which is empty. At the bottom right, there are two buttons: '>> Next' and 'Cancel' with a red X icon.

- 17 Click **Next** on the **Reset System Operator** window.



The 'Schlage SMS Login' dialog box is shown. It has a blue title bar and a light beige background. On the left, there is an icon of a computer with a monitor and keyboard. The main area is titled 'Schlage SMS Login' and contains the following text: 'Shown here is the login and password used by Schlage SMS to log onto the SQL Server. This account should have administrative privileges over the selected database and adequate privileges to add and delete users from the system.' Below this text are three input fields: 'Login Name:' with the value 'SMSAdmin', 'Password:' with a masked value 'XXXXXXXXXX', and 'Confirm Password:' with a masked value 'XXXXXXXXXX'. At the bottom right, there are three buttons: '<< Back', 'Next >>', and 'Cancel' with a red X icon.

- 18 Click the **Finish** button.



- 19 You may open and use the **Schlage SMS** software.

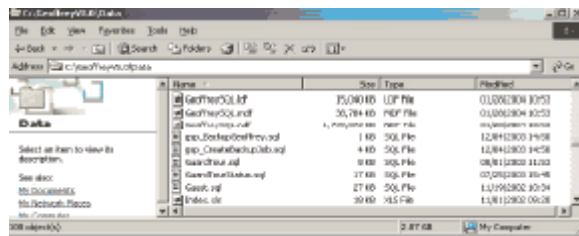
Appendix B: File Space Monitor

Introduction

All systems that use Microsoft Data Base Engine (MSDE) have an inherent file size limit of 2 GigaBytes (GB). Those **Schlage SMS** software versions that have been installed with MSDE (Microsoft Data Base Engine), will have this file size limit (2,097,152 KB) for the SchlageSQL database. This section of the document describes the areas in the **Schlage SMS** system affected by this limitation, and the **File Space Monitor** utility that monitors and controls the file size.

Data file utilization in Schlage SMS

The SchlageSQL database contains three files: **Schlage.LDF**, **Schlage.MDF** and **SchlageSQL.NDF**. Total file size of the **SchlageSQL.MDF** and **SchlageSQL.NDF** should not exceed the 2 GB limit. The file size of **SchlageSQL.LDF** does not count towards the 2 GB limit. To determine the file size go to your system and select the **Schlage\Data** folder and get the file size for these three files.



Name	Size	Type	File Offset
SchlageSQL.Ldf	15,040 KB	LDF File	013062704 30751
SchlageSQL.Mdf	38,784 KB	MDF File	013062704 30751
SchlageSQL.Ndf	1,739,072 KB	NDF File	013062704 30751
SchlageSQL.Ldf	1 KB	SQL File	12,841,030 34,038
SchlageSQL.Mdf	4 KB	SQL File	12,841,030 34,038
SchlageSQL.Ndf	8 KB	SQL File	08,811,030 34,038
SchlageSQL.Ldf	27 KB	SQL File	02,046,030 34,038
SchlageSQL.Mdf	27 KB	SQL File	11,996,030 34,038
SchlageSQL.Ndf	39 KB	SQL File	11,911,030 34,038

From the sample shown above, the file size of the above mentioned files are given below. We will be using these values throughout this document.

- SchlageSQL.Ldf 15,040
- SchlageSQL.Mdf 38,784
- SchlageSQL.Ndf 1,739,072

Add the **SchlageSQL.MDF** and the **SchlageSQL.NDF** and we come up with the total size for your **SchlageSQL** database. 1,792,110 KB.

When the total of these two files reach the 2 Gigabytes limit, one of two things will happen to the **Schlage SMS**.

- 1 If the **SchlageSQL.NDF** is the file that has been completely allocated and all space has been used, all transactions that are being received from the RC network will not be written to the **SchlageSQL.NDF** file and will be discarded. The on-line monitor will no longer display transactions and alarms will no longer be received.
- 2 If the **SchlageSQL.MDF** is the file that has been completely allocated and all the space has been used, database records will be entered into the Schlage Access database, but they will not be saved in the **SchlageSQL.MDF** file. These database entries will be discarded.

Resolution

To monitor and limit the growth of the SchlageSQL files, **IR Security Technologies** has created a program called the **File Space Monitor** (FileSpaceMonitor.exe). This program is designed to reduce the system file size, if this limit has been reached and to prevent the system from reaching this limit in the future.

The following programs are provided on the CD

- 1 DatabaseMaintenanceUtility.exe
- 2 FileSpaceMonitor.exe
- 3 QR.exe

The following steps should be used to determine the status of your **Schlage SMS** file sizes, and make the proper adjustments accordingly.

Step 1

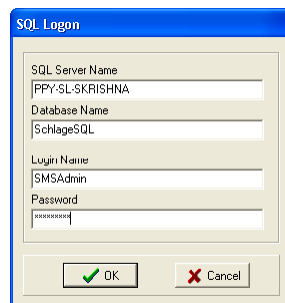
Prior to performing any of the following tasks, please shutdown the entire **Schlage SMS** software on all servers, and workstations.

Step 2

Copy all three files provided from the CD onto the Server or Single User Workstation and place them into the Schlage\Bin folder.

Step 3

- 1 From the Schlage\Bin folder, double click on the **FileSpaceMonitor.exe** program.
- 2 You are prompted to login to the SQL database. SQL Server Name, Database Name, and Login Name fields are automatically populated. Enter your password in the Password field. Click **OK**.



SQL Logon

SQL Server Name
PPY-SL-SKRISHNA

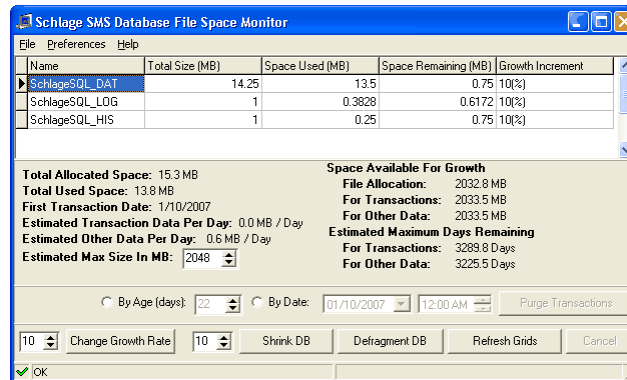
Database Name
SchlageSQL

Login Name
SMSAdmin

Password
[Empty]

OK Cancel

- 3 The following window is displayed. For the purposes of this document, we are using our in-house test system to display results. Your values may differ.



Explanation of terminology

- 1 **Total Allocated space** - This is the total amount of hard disk space used by the **SchlageSQL.MDF** and **SchlageSQL.NDF** files. These sizes are displayed when viewing the files in "My Computer" or "Windows Explorer". The 2 GB size limit refers to this total.
- 2 **Total Used space** - Only a portion of the allocated space contains Schlage SMS data. Another portion is kept empty to allow new Schlage SMS data to be quickly recorded onto the hard disk. This empty space will be gradually filled as transactions, cardholders, and other data are added to the system. When the used space grows to fill all of the allocated space, SQL server increases the allocated space by 10%, and the process begins again.

Explanation of File Space Monitor Program Items

- 1 On the top half of the screen, you will see six columns.
 - a) **Name** - This column displays the names of the three files that comprise Schlage database. They are listed here as
- 2 SchlageSQL_DAT, (SchlageSQL.MDF). SchlageSQL_LOG, (SchlageSQL.LDF) and SchlageSQL_HIS (SchlageSQL.NDF)
 - a) **Total Size (MB)** – This column is the total allocated size for each of the three SchlageSQL files. Allocated space includes both valid data and empty space that has been reserved to allow new data to be written to disk quickly.

For example: When the **SchlageSQL_DAT** file was created, the allocated file limit was around **11,000 KB**. This file will be empty when it was created and had a space for **11,000 KB** of data that could be filled until the file was full. When this file became full with data, the file size would be increased by **10%** to allow for future growth. The allocated space for this file would increase by **10%** and now be at: **12,100 KB**. This increase of 10% each time the file size grows and fills up the empty space will continue as the **Schlage SMS** database increases. This same growth and allocation happens to the **SchlageSQL_HIS** file as the RC panels in the field sends back transactions and alarms. In our example: SchlageSQL_DAT = 41.685

- SchlageSQL_LOG = 14.6875
- SchlageSQL_HIS = 1698.3125

- a) **Spaced Used (MB)** – This column shows the amount of space that has been used from the total amount that was allocated from the previous column for each file. Keep in mind that the total allocated file size is the amount that has been allocated for growth with 10% remaining for growth. Space used is now showing how much space has really been used for storage of history and data. For example the **SchlageSQL_HIS** has used up **863.5625 MB** of the total amount allocated to store transactional history. In our example:
- SchlageSQL_DAT = 37.75
 - SchlageSQL_LOG = 3.6016
 - SchlageSQL_HIS = 863.5625
- a) **Space Remaining (MB)** – This column shows the amount of space remaining for growth before each file will be allocated another 10%. For example the **SchlageSQL_HIS** has another **835.75 MB** of file size remaining prior to the file being reallocated by another 10% In our example:
- Schlage SQL_DAT = 3.9375
 - SchlageSQL_LOG = 11.0859
 - SchlageSQL_HIS=835.75
- a) **Growth Increment** – This column shows the file size growth limit that was set for each file during the installation.
- 3 In the middle of the screen, two sections will be displayed with pertinent information regarding your system.
- a) **Total Allocated Space** - 1740.0 MB – This is the combined total allocated space for **SchlageSQL_DAT** and **SchlageSQL_HIS**. The **SchlageSQL_LOG** file size does not get added into this total.
- b) **Total Used Space:** 900.3 MB – This is the combined total used space for **SchlageSQL_DAT** and **SchlageSQL_HIS**. The **SchlageSQL_LOG** file size does not get added into this total.
- c) **First Transaction Date:** 04/28/2003 – This is the first transaction that has been stored on this in-house test system.
- d) **Estimated Transaction Data Per Day** - 3.0 MB / Day – This amount is calculated by dividing the total used space of the **SchlageSQL_HIS** file by the number of days since the first transaction.
- e) **Estimated Other Data Per Day** - 0.1 MB / Day – This amount is calculated by dividing the total used space of the **SchlageSQL_DAT** file by the number of days since the first transaction.
- f) **Space Available For Growth**
- File Allocation - 308.0 MB** - To come up with **308.0 MB**, we took the **2048 MB** limit and subtracted SchlageSQL_DAT size of **41.6875 MB** and then subtracted the SchlageSQL_HIS size of **1698.3125 MB** and this gave us: **308.0 MB** for allocation growth. This is how much space could be allocated for growth, prior to our inhouse **Schlage Security Management System** running out of allocation space for either transactional history or database entry.
- For Transactions - 1143.8 MB** – We take the total file allocation of **308.0 MB** remaining for growth, and take the empty space for the **SchlageSQL_HIS** of **835.75 Megabytes** that transactions can be stored in and we come up with **1143.8 Megabytes** remaining for transactional storage.
- For Other Data - 311.9 MB** – We take the total file allocation of **308.0 MB** remaining for growth, and take the empty space for the **SchlageSQL_DAT** of **3.9375 Megabytes** that database data may be stored in and we come up with **311.9 MB** remaining for data base data.
- g) **Estimated Maximum Days Remaining**
- For Transactions - 375.6 Days** – This limit is calculated by dividing the Total File Space Available for Growth for Transactions (**1143.8 MB**) by the Estimated Transaction Data Per Day (**3.0 MB/Day**)

For Other Data - 127.9 Days - This limit is calculated by dividing the *Total File Space Available for Growth for Other Data (311.9 MB)* by the *Estimated Transaction Data Per Day (0.1 MB/Day)*

- The bottom third of the screen has functions that the end user will need to use to maintain the proper file sizes of the **SchlageSQL**. We are going to explain this portion at a later point.

Examples of Schlage SMS in the field

Example 1:

We have installed the **File Space Monitor** Program, and for example we have noted that under the **Caption: Estimated Maximum Days Remaining** under the heading: **For Transactions:** We see **375.6 Days**. What this means is at the rate of growth for history storage, your system will reach the **2 Gigabytes** file limit in approximately **375.6 days**. **At that point**, transactions will no longer be stored, and alarms will no longer be displayed. (Refer to Figure 2) Close the File Space Monitor program and proceed to **step 4**.

Step 4 - Backup Database

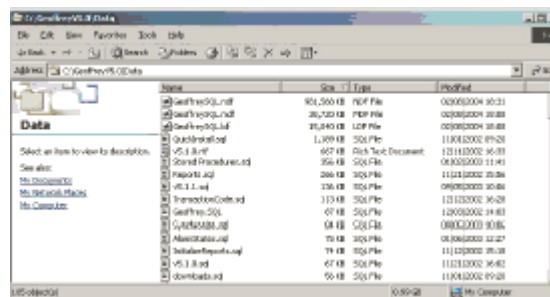
Refer to the **Database Maintenance Utility** documentation for further information on backing up the database.

Note: At this point please verify that under the **Schlage\Data\Backup** folder that a file in the format of **20040208.bak** now exists. (The year, month and day will vary) This will be the completed backup of the SchlageSQL file that the Database Utility just performed.

This new Database Maintenance Utility program will also perform the command: **Shrink Database on the SchlageSQL**. What this means is that after the backup of the SchlageSQL has been completed, the utility will remove all of the unused space that has been allocated as the system has been running and bring down the total of allocated space to the 10% that has been setup for the growth of the files. This may free up some space for your system to store history. The File Space Monitor Program will reflect this change.

Now you should also go back into the **Schlage\Data** folder and look at the file sizes of the three SchlageSQL files.

Refer to the screen display below. The Database Maintenance Utility Backup has reduced the file sizes dramatically.



Name	Size	Type	Modified
SchlageSQL.ndf	824,500 KB	NDF File	02/08/2004 10:21
SchlageSQL.log	38,743 KB	LOG File	02/08/2004 10:28
SchlageSQL.trn	35,343 KB	TRN File	02/08/2004 10:28
SchlageSQL.bak	1,009 KB	SQL File	11/04/2002 19:28
v5.1.1.rtf	607 KB	Rich Text Document	12/14/2002 16:01
Stand Procedures.rtf	356 KB	SQL File	08/02/2002 11:41
Procedures.rtf	246 KB	SQL File	11/14/2002 10:06
v5.1.1.rtf	326 KB	SQL File	08/02/2002 10:06
TransactionControl	113 KB	SQL File	12/12/2002 16:28
SchlageSQL	67 KB	SQL File	12/02/2002 14:43
SchlageSQL	68 KB	SQL File	08/02/2002 10:06
Allocations.rtf	79 KB	SQL File	08/02/2002 12:27
SchlageSQL.rtf	79 KB	SQL File	11/12/2002 10:06
v5.1.1.rtf	67 KB	SQL File	11/12/2002 16:01
download	55 KB	SQL File	11/04/2002 19:28

Step 5

- Select the **Schlage\Bin** folder and double click on the **FileSpaceMonitor.exe** program.

- 2 After performing the database backup, we have noted that our top column data and our total **Allocated Space and Space Available For Growth** and **Estimated Maximum Days Remaining** have changed. These changes are not the same for each system and your data may or may not have changed after the **Data Base Maintenance Utility Backup** was performed.

Note: You may or may not have achieved your attempted goal for Estimated Maximum Days remaining For Transactions prior to the Max File size limit of 2 gigabytes has been reached by performing the **Database Maintenance Utility** Backup. Keep in mind that most of the free space remaining was removed and the next file size allocation may put you back in the same condition as far as disk space that was used prior to the backup.

- 3 Let us continue with the explanation of the **File Space Monitor** Program. At the bottom third of the screen are two rows of information along with featured buttons and other user functions. This portion of the program is designed for the user to know how many days are available for the system to run at the current rate of history and database growth prior to reaching the max file size limit of 2 Gigabytes.
- 4 The Row that has: **By Age (days): 287 By Date: 04/28/2003 12:00 AM Purge Transactions**. This row was created to satisfy a need of the **Schlage SMS** with software versions 5.06B and below that does not have **History Archiver** program incorporated. These versions will not be able to archive out any history from the **SchlageSQL_HIS** file to gain space for storage. The only option in these versions will be to purge the transactions. All purged history will be deleted permanently from the system and no reporting capabilities will be available for these transactions. When bringing up the **File Space Monitor** program on a **Schlage SMS** using version 5.0.6B or less, you may need to use this section of the program to purge some of the current history that has been stored to free up disk space if the total of the two SchlageSQL files is near the file size limit of 2 Gigabytes. Because there is no **History Archiver** in these versions of software, we have provided the user with two options as to how to purge transactions from the system.

Option 1: By selecting **By Age (days)**. The system populates the default value in this field based on the day of the first transaction that occurred in the system. The default value for the test system used here is 287. The neighboring spin box and **Purge Transactions** buttons will now be enabled. The program is now telling the user that 287 Days of history are stored in the file **SchlageSQL_HIS**. The user can now determine how many days of history that is currently stored in the database need to be deleted. By entering in the value 257, the system will calculate how many transactions have been stored in the last 30 days in the **SchlageSQL_HIS** and notify the end user of the total amount of transactions that will be purged when selecting the **Purge Transactions** button.

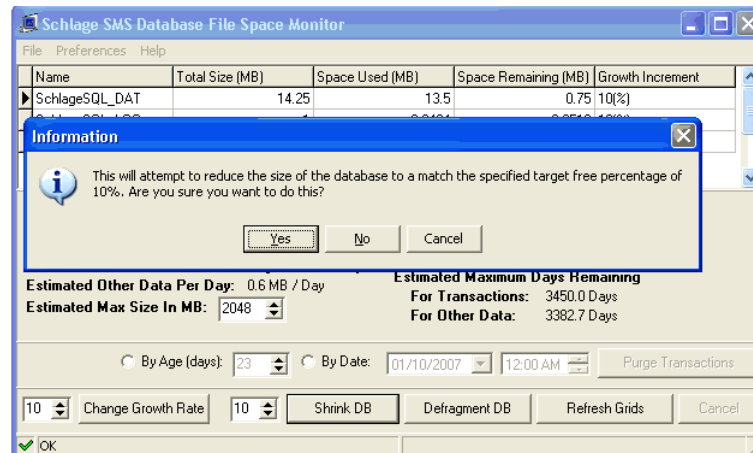
Option 2: By selecting **By Date**: For this example the field defaults to 04/28/2003 12:00. That is the date of the first transaction occurred in the system. The **Purge Transactions** button will also become enabled. The program is now telling the user that the first transaction stored in the **SchlageSQL_HIS** file is from 04/28/2003 at 12:00 AM. The user needs to use the specific date and time for the system to purge transactions to meet the specified date. By selecting the date of 05/28/2003, the system calculates how many transactions have been prior to that date and notify the user of the total amount of transactions that will be purged when selecting the **Purge Transactions** button.

- 5 After determining which method of the **Purge Transactions** you are using, select the **Purge Transactions** button and let the utility perform the action. We have noted in our testing of this program that, if your system receives an average of 30,000 transactions per day, and you select 30 days to purge; this range to purge will take approximately 10 minutes. After the purge has completed, on the second row of the bottom third of the utility is a button labeled: **Update Statistics**. Selecting this button after the purge has completed or after any operation of the **File Space Monitor Utility** has been performed will update the data in the top two thirds of the screen.
- 6 The last row of **File Space Monitor Utility** has 4 operations that we will now explain.
 - a) **Change Growth Rate** – This refers to the growth of the file allocation size. The default for this item is 10%. This indicates that the next time additional space is allocated by MSDE; it will be done in an increment of 10%. **Ingersoll Rand** recommends that this setting not be changed unless you have contacted our support department for assistance.

- b) **Shrink DB** – This refers to the portion of the allocated space that should be kept empty. The default for this item is 10%. This rate could be changed if needed.

Note: It is highly recommend that this setting not be changed unless you have contacted **Ingersoll Rand** support department for assistance.

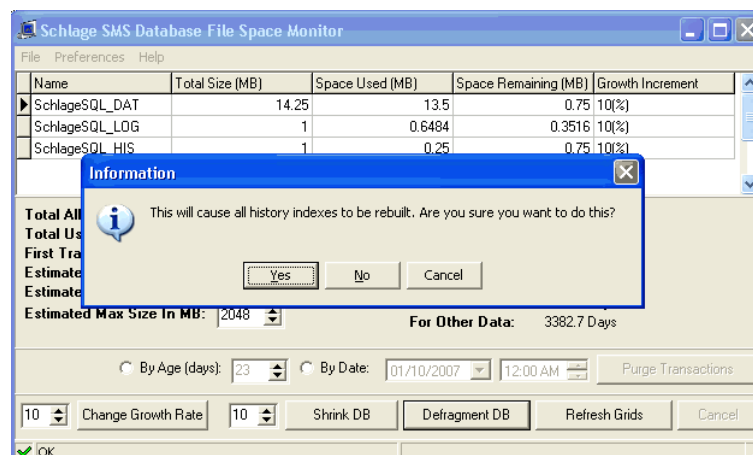
- 7 The **Shrink DB** button will evaluate the amount of empty space remaining and attempt to adjust it to match the percentage specified. For instance, if the database has 900 MB of space used and 300 MB of space empty (for a total allocation of 1200 MB), pushing this button will reduce the empty space to 100MB (for a total allocation of 1000 MB). When you select the Shrink DB option you will receive the following screen:



- 8 A message will be displayed stating that this program will attempt to reduce the size of the database to match the specified target free percentage of 10%. If you select **Yes**, a message and progress bar will be displayed in the status bar at the bottom of the window.
- 9 **Defragment DB** - All SQL Server databases, over time, experience "internal" fragmentation of its data. This occurs when records are removed from database pages, but the space it occupied is still there after deletion. Eventually this space is reused, but as it is reused, the data pages become physically fragmented. This fragmentation causes the system to run slower as far as running reports and getting system data changes out to the controller network.

Defragment DB option optimizes the database and history indexes that exist. The optimization will actually delete the existing indexes and re-insert and rebuild new ones. This will increase the allocated size of the SchlageSQL.MDF and SchlageSQL.NDF by 1/3 to 1/2 of the original size when completed.

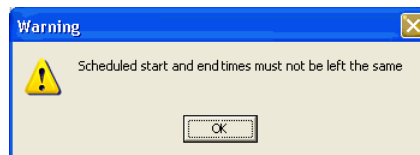
- 10 When performing the Defragment DB program, you will receive the following display.



Schedule Preferences

Options to schedule Purge Transactions, Shrink Database and Defragment Index are available under the **Preferences** menu.

- 1 Select the **Enable Scheduling** option to enable the choices in this window.
- 2 Enter the the description for the **Job Owner**. The Job Owner must be the database administrator.
- 3 Next, select the time and date for performing the scheduled jobs.
 - a) **Every...minutes** - Enter the interval at which you want run the selected procedures. Fifteen (15) is the default value. Adjust the value using the up and down arrows, or enter manually. If the start and end time are the same, you will see the following error message.



Select the time period to run the procedures.

- b) Select the days by checking the checkboxes next to the days.
- 4 **Purge Transactions** - Perform this task to free up space in the database or to delete obsolete information. You can choose to purge performance data based on the age of the transaction.

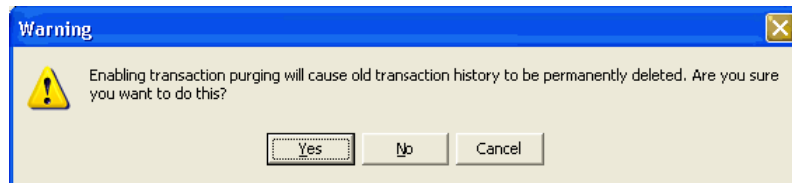
Select the check box to enable the **Purge Options**. There are two methods of purge transactions available.

- a) **By Age** (days) - The default value is 365. By setting the value to 365, the system is telling the user that, 365 days of history is stored in the database. It will calculate the number of transactions occurred prior to the set days, and notify the user of the total number of transactions that will be purged. You can change the number of days by using the up and down arrows or you can type in the value.

Purge Transactions By age (days) option is also available in the bottom part of the main window of File Space Monitor. There, By Age (days) field is automatically populated with the number of days of history currently stored in the file **SchlageSQL_HIS**.

- b) **By Date** - All the transactions occurred prior to the specific date and time set here will be purged.

- c) **Locking Type** - The locking type means how the database locks the record that is currently being used. The choices are page Lock (paglock), row lock (rowlock), and table lock (tablock). Default choice is paglock.
 - d) **Maximum rows to purge at once** - Here you can specify the number of rows in the database that will purge at once.
- 5 **Shrink DB** - Select the Shrink DB check box to enable this option. This refers to the portion of the allocated space that should be kept empty. The default for this item is 10%. This rate can be changed if needed. Enter the required percentage in the **Percentage free space** field.
-
- Note:** It is highly recommend that this setting not be changed unless you have contacted **Ingersoll Rand** support department for assistance.
-
- 6 **Defragment Indexes** - Selecting this option will attempt to defrag all transactional and database indexes that have been created in the SchlageSQL files. When the system is installed, indexes have been created for Cardholders, Areas, Area Sets and all History. As the system runs over a period of time, these indexes become fragmented. This fragmentation will cause the system to run slower as far as running reports and getting system data changes out to the controller network. Defragment Index option will perform a process that optimizes all of the database and history indexes that exist. The optimization will actually delete the existing indexes and re-insert and rebuild new ones. This will increase the allocated size of the SchlageSQL.MDF and SchlageSQL.NDF by 1/3 to 1/2 of the original size when completed.
- 7 Click **Save and Exit** to schedule the job. These settings will replace any existing job schedule. You will also see the following warning.



Schlage SMS field problems and solutions

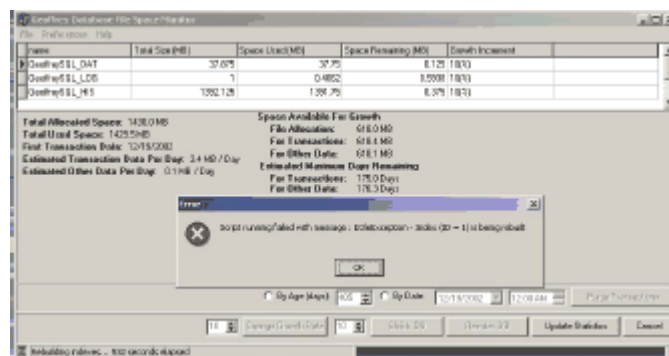
Now that we have described all of the functions of the File Space Monitor, let us describe a few scenarios that may arise in the field and solutions.

Scenario 1: - SchlageSQL.NDF too large in size to perform Reindex DB

On your **Schlage SMS**, you determined that you were going to either purge or Archive your transactions and get the system so the statistics are within the desired range for growth.

You have noticed that the reporting seems to be running slower than they were in the beginning and you would like to improve the performance. You decide to Reindex the DB.

You select the Reindex DB button and the Rebuilding Indexes message is displayed at the bottom of the screen for some amount of time. In our in house test system, this was 532 seconds. Then you receive a message similar to the one displayed below.



Let us discuss what has happened. Look at the second Column. Total Size (MB) for SchlageSQL_HIS. The file size was 1392.125 (This is approximately 1.4 Gigabytes). In the earlier explanation of the Reindex, we stated that this process uses a substantial amount of allocated space to perform this procedure. There are approximately 30 indexes that get rebuilt during this process. The error message is saying that this process has failed during the rebuild of one of these indexes. While the rebuild was being performed, we reached the 2 gigabyte file size limit and ran out of room to complete the Reindex process.

The SQL software will perform what is called a rollback, and after you click on the **OK** message, your system will be back at the same file sizes and performance that was encountered prior to attempting the Reindex DB.

We have found through our in-house testing that in order to run the Reindex DB you may need to bring down the size of the SchlageSQL.NDF to approximately 1,122,816 MB.

In order to get the file size down to approximately the 1,122,816 MB, you need to accomplish two of the following.

- a Using the File Space Monitor program, use the Purge Transactions (Software versions 506B or below) and then perform the **Shrink DB** function of the **File Space Monitor**. In order to Decrease the amount of *Months of Online History* that the **History Archiver** will allow the end user to run current reports on and manually start the archiving process. When completed, using the **File Space Monitor** program, perform the **Shrink DB** function.
- b When making the decision to perform the Reindex DB function of the File Space Monitor program, if your SchlageSQL.NDF file is above the recommended limit, you may try the Reindex DB first prior to the steps above. The only downside of running the **Reindex DB** option of the **File Space Monitor** program and having it fail will be the time that has been used in attempting the Reindex.

Scenario 2: - Shrink DB or Reindex DB not performing properly

During our in-house testing, we have noted one problem with the **Shrink DB** and the **Reindex DB** operations.

Problem: When running the **Shrink DB** operation immediately followed by a **Reindex DB** or Vise Versa, we have found that the second operation may tell you that the operation has been completed either in 0 seconds and no change has been made to the **SchlageSQL files** or the operation may have taken some time to perform but again, no change has been to the **SchlageSQL files**. This occurs because MSDE requires time to update its statistics tables, which are used by the Shrink DB operation.

Solution: After performing a **Shrink DB**, wait approximately **30 minutes** before running the **Reindex DB** and Visa Versa.

Files and documents included in this package

- 1 Database Maintenance Utility.exe
- 2 FileSpaceMonitor.exe
- 3 QR.exe
- 4 **Schlage SMS** with MSDE documentation

Appendix C: Database Maintenance Utility

Introduction

This utility is used to backup the database and to archive history files. It will also perform a complete **Defrag** and **Re-index** of all SchlageSQL tables and a complete Purge of all records that have been scheduled for deletion. These functions can be run manually from the Tools menu, or they can be scheduled to run automatically. This section details the various functions of the utility and gives instructions on how to set up the utility and schedule regular maintenance.

Requirements

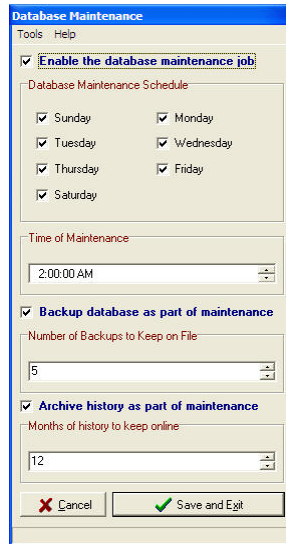
The Database Maintenance Utility can be used on systems installed with SQL 2000 (with service pack 4), MSDE 2000 (with service pack 4), SQL 2005 with service pack 3 (full and express) and SQL 2008 (with service pack 1). If using full version of SQL or MSDE then **SQL Agent** will be available. If using express version of SQL then **Windows Task Scheduler** will be used.

Accessing the application

- 1 You can start Database Maintenance Utility from the **System Launcher** or go to **Start>Programs>Schlage SMS>Database Maintenance Utility**.

Note: When the utility is started from the System Launcher, the database cannot be restored from the backup as the database is still in use. When the application is started from the desktop, the **Restore Database** option is available from the Tools menu.

Overview



When the Database Maintenance Utility is run for the first time, the initial **Schlage SMS Database Purge Job** may take some time. Depending on the size of your database and history files, the **Purge and DBCC Defrag Index** process may take up to four hours or more to complete.

When a database is restored, you must run the **Recreate Purge Procedures** from the Database Maintenance utility in order to get the **Schlage Database Purge** procedures set back up properly.

Prior to running the Database Maintenance Utility, please make sure that the **PURGE.SQL** file that resides in the **Schlage SMS\Data** folder has not been set to **Read Only**. If this attribute has been set in this manner, please remove the Read Only attribute so you do not receive any error message when the PURGE.SQL is set to be installed.

Note: You need to assign appropriate security privileges to operator's in order to prevent unauthorized users from performing backup and restore procedures. Essential options are available only operators with Read/Write or Administrative permissions.

This utility will not perform a backup on the AlarmStateSounds, Graphics, Instructions, Launcher Graphics, Maps, Portraits, or Signatures folders under the Schlage SMS\Data folder. These folders should also be backed up or copied to another media periodically to preserve the data in case of recovery.

Once the database has been backed up using the Database Maintenance utility, the SchlageSQL backup files should also be copied to another media in case this backup is required due to any hardware failure and will be required for recovery.

Installation and set-up

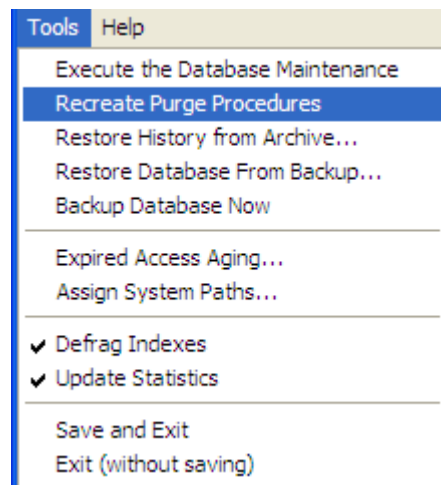
When installing the Database Maintenance Utility it should be accessed from **Start>Programs>Schlage>Database Maintenance**.

- 1 **SQL Logon** - The first screen you see when you open the **Database Maintenance Utility** is the SQL Logon. The SQL Server Name the Database Name and the SQL Login fields will already be populated with the correct information. This allows you to establish a connection with the SQL Server. Then enter the the Password and click **OK**.

Note: If you are running Database Maintenance Utility from the System Launcher, this step will be skipped.

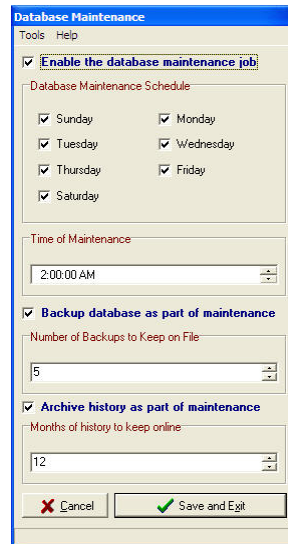


- 2 Once you have logged in successfully select **Tools>Recreate Purge Procedures** from the Database Maintenance Utility window. This utility will investigate all dependencies on tables in order to configure itself.

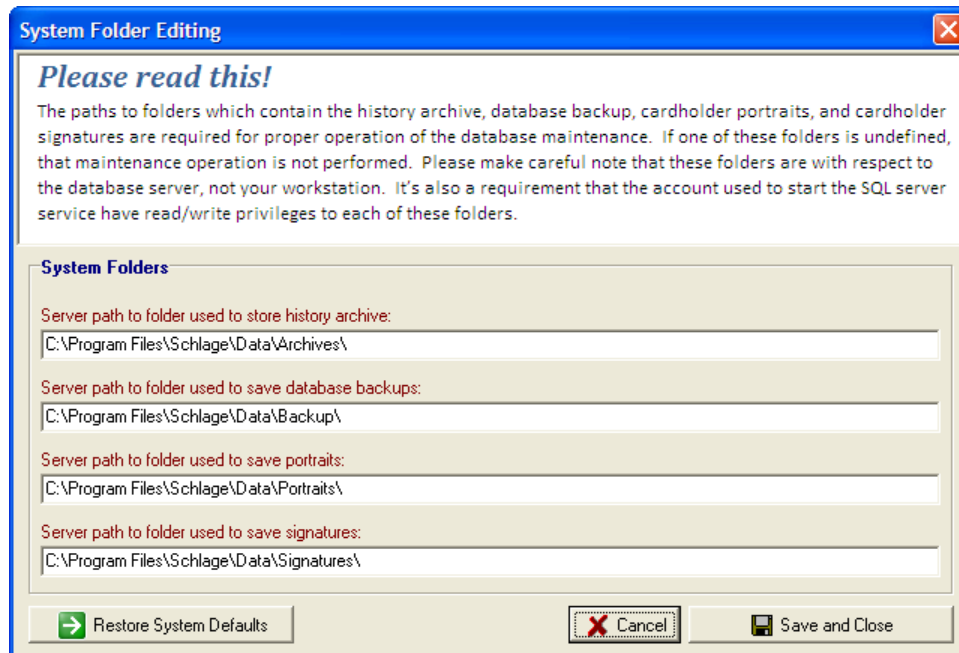


- 3 This procedure will then determine what version of **Microsoft SQL** is running.
- 4 Finally the proper **PURGE** procedures will then be installed onto the system.
- 5 The Database Maintenance Utility will be used to setup an SQL Agent Job (or Windows Task) that will automatically perform all procedures selected by the end user. There are 5 items that may need to be setup by the end user.

- a) **Enable the database maintenance job** - When the **Schlage SMS Database Purge** job has been setup, this check box enables or disables the SQL Agent Job. This feature must be checked in order for the SQL Agent to perform the job. Disable the job by leaving this unchecked.



- b) Next step would be to select the **Database Maintenance Schedule**- This operation would enable the days that the SQL Agent Job will be performed.
- c) Next step would be to pick the **Time of Maintenance** - This operation would enable the time that the SQL Agent Job will be performed. Review all other Jobs that might be scheduled and have this Job performed at a different time than others. Preferably at night when the system is not busy.
- d) Next step would be to select **Backup database as part of maintenance** - This determination may need to be discussed with your IT department. A complete backup of your database may be already being performed and this operation of the Database Maintenance utility may not need to be selected.
- e) Next step would be to select **Archive history as part of maintenance** - This new option replaces the Archive application. Check this option to archive history every time the Database Maintenance Utility is run.
- f) If determined that the Database will be a part of the Database Maintenance utility, next step would be to determine the **Number of SQL Backups to Keep on File**.
- 6 The **Database Maintenance Utility** will backup the database, archive the history files and remove any photo or signature files that are no longer associated with cardholders. In order to accomplish these tasks the destination folders of the specified files need to be defined. The system folder editing tool is used to achieve this. To access this option go to **Tools>Assign System Path**.



The **Restore System Defaults** button can be used to restore default values. **Note:** If one of these folders is undefined, that maintenance operation is not performed.

- 7 The database will be backed up in the following format:

SchlageSQL_20051111094538.bak – The first 4 digits are the year (2005), followed by Month and Day (1111), followed by hours (0945) and seconds (38).

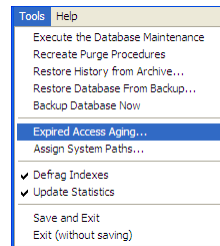
- 8 The **Database Maintenance Utility** will remove the oldest backup prior to performing a new backup when the set limit of backups has been reached.
- 9 When all data entries have been made, click on the **Save and Exit** button to create the scheduled job. The utility will then close automatically.
- 10 To verify that the job was properly setup, bring up the Database Maintenance utility again. Review and make sure that all of the previous selected data is now displayed. This verifies that the job was created. On a full version of SQL you may now go into the SQL Agent and under Jobs, select the **Security Management System Database Purge** and review the steps that are being performed.

Operation performed by the SQL Agent

- 1 The SQL Agent will now perform the **Security Management System Database Purge** automatically using the pre-selected days and time that was setup via the Database Maintenance utility.

Note: The Database Maintenance Utility now performs a purge of portraits and signatures when cardholder records are deleted from the database. The portraits and signatures are not deleted until the cardholder records are physically deleted from the database as opposed to being tagged as deleted.

- 2 The database maintenance utility also purges expired access privileges. Select **Tools>Expired Access Aging** to set the number of days to keep the privileges after they are expired.



- a) To enable this feature check the **Enable deletion of expired privileges** check box. If left unchecked this feature will be disabled. The **Set Aging of Expired Access Privileges** window opens. Enter the value in the **Number of days to hold expired access privileges** field. If the field is set to one (1) then expired area access records are preserved for one day (24 hours from expiration date\time) and then deleted from the database.



Manual operation of the Database Maintenance Utility

To manually operate the **Database Maintenance Utility**,

- 1 Select **Tools>Execute the Database Maintenance**. This will execute all of the user-selected settings for Purging, Defrag Indexing and Backup procedures.

Note: All options in Database Maintenance Utility will be disabled while the manual job is running. This may take as long as an hour to complete. When the options are enabled, the job is complete.

- 2 Verify that the backup completed successfully: go to the Schlage\Data\Backup folder. There will be backup files with the current date if the backup was successful.

Database maintenance procedures for restoring the database

The **Database Maintenance Utility** can be used to restore the Schlage SQL database. There are a few reasons why you might want to use this utility to perform a complete restore of the database.

Note: When the program is started from the System Launcher, the database cannot be restored from the backup as the database is still in use. When the application is started from the desktop, the restore database option is available from the Tools menu.

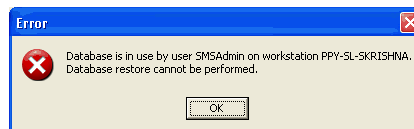
One reason would be a catastrophic failure like a hard disk failure or SQL corruption. In this case, the once the Operating system as well as the Microsoft SQL application has been restored to the hard drive, a clean installation of the Schlage SMS would then need to be performed. Then the Database Maintenance Utility could be used to restore a backup with all of the data and history.

Another reason may be that some major database changes have been made and we have decided to restore back to an earlier set of data prior to those changes.

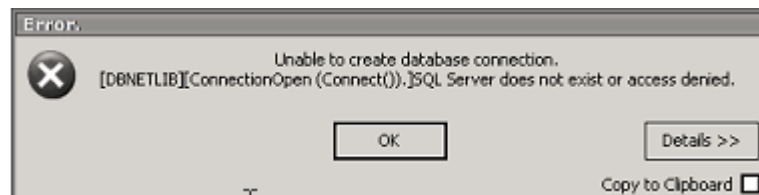
If the SchlageSQL database has become corrupted, you may need to get an IT person involved to correct this problem, or a complete re-installation of the software may need to be performed. The Database Maintenance Utility may then be used to restore a backup once the original SchlageSQL database has been corrected.

Manual operation to restore a backup of the SchlageSQL

When performing the restore of the SchlageSQL database, please ensure the entire **Schlage SMS** software has been shutdown or you will receive the following error message.

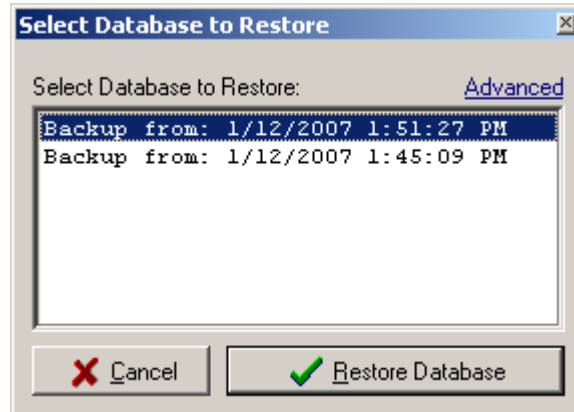


Prior to launching the Database Maintenance Utility, ensure that the SQL database is running or you will receive the following error message.

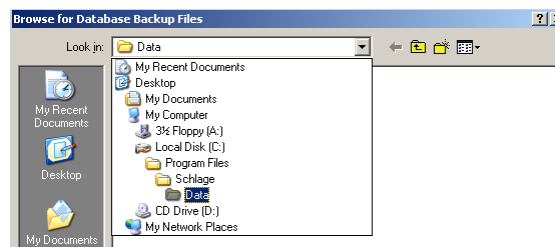


- 1 To restore a SchlageSQL database, launch the **Database Maintenance Utility** and from **Tools** menu, select **Restore Database From Backup**.

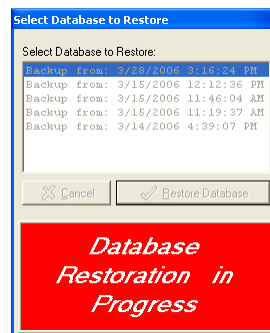
- 2 You will now see a **Select Database to Restore** window. All backups from the Database Maintenance Utility will be displayed. Select the backup that will be restored and click on the **Restore Database** button to continue.



If you want to browse to for database backups, click on the **Advanced** option. This opens the **Browse for Database Backup Files** window. Select the backup file, and click **Open**. The default folder for Schlage SMS backups is C:\Program Files\Schlage\Data\Backups.



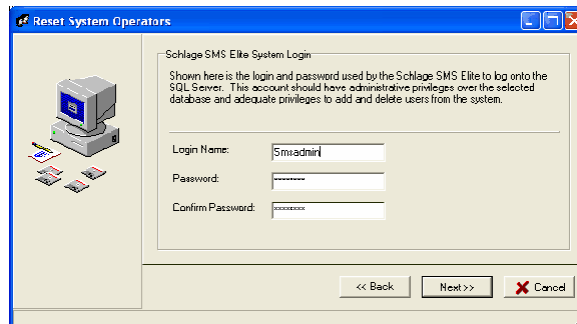
- 3 The **Database Restoration in Progress** message will now be displayed.



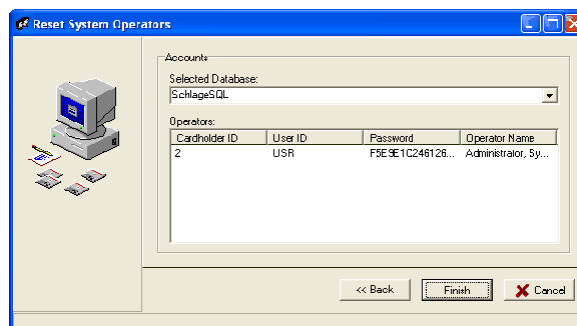
- 4 When the restoration is complete, **Restore Users** procedure will be performed. Tab down to the **Password** selection and enter in the password for **sa**. Unless this has been changed by the IT personnel, this password should be: **SECAAdmin1**. When completed with the entry, click on the **Next** button to continue.



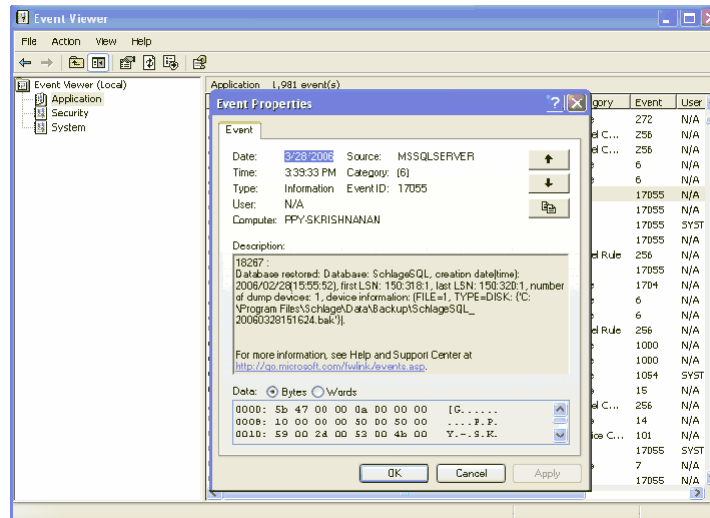
- 5 The next screen displayed will be the **Reset System Operators**. Please accept the defaults and click on the Next Button.



- 6 The next screen displayed will be another **Reset System Operators** screen that will display all of the operator logins that exist in the SchlageSQL database. Click **Finish** button. To complete this process may take several seconds depending on how many operators exist in your database.
- 7 When complete, this screen display will be removed from your screen and the restore procedure has now been completed. You may now launch the System Launcher and verify your data and overall operation of the Security Management System.



You may also review any error messages pertaining to this recovery task in the Windows, **Event Viewer** under the **Application Log** tab.



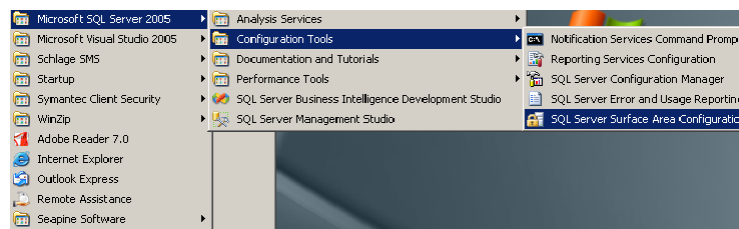
Appendix D: MSSQL 2005 Server Configuration Settings

Introduction

Schlage SMS Version 5.2 and higher support the use of SQL 2005 Standard and Enterprise editions. SQL 2005 Express is not supported. The following settings must be adjusted in a SQL 2005 Standard/Enterprise installation in order to support the software.

Settings

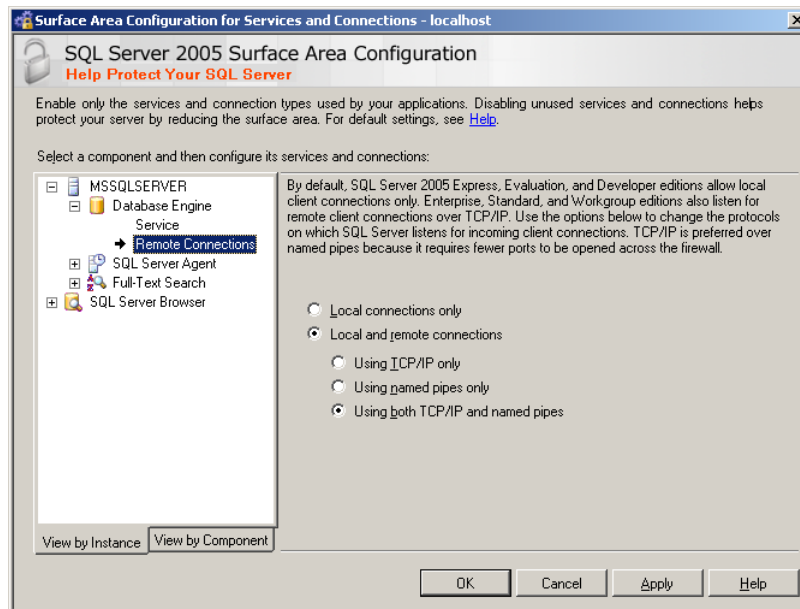
- 1 Several Settings in the SQL Server Surface Area Configuration must be enabled. Go to **Start>Programs>Microsoft SQL Server 2005>Configuration Tools** and select **SQL Server Surface Area Configuration** menu item.



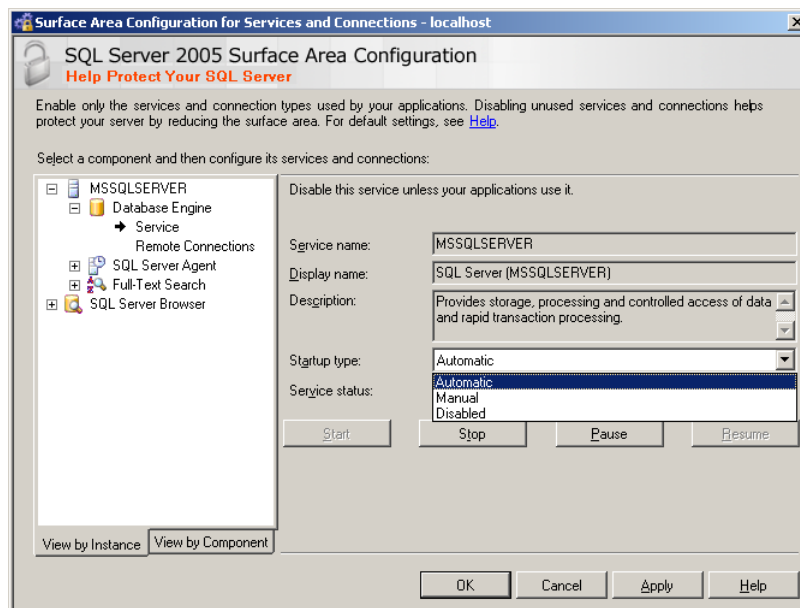
- 2 Click the **Surface Area Configuration for Services and Connections**.



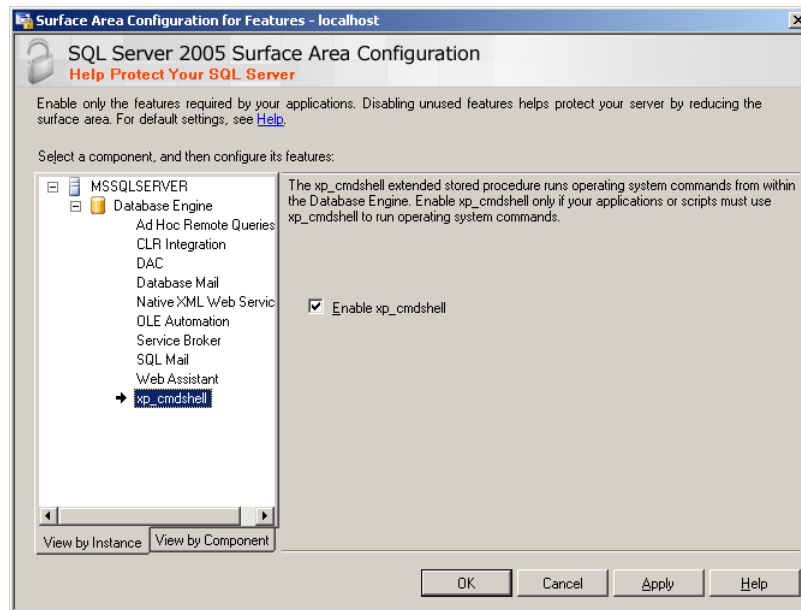
- 3 Under **Database Engine**, select **Remote Connections**. Enable “Local and remote connections” and “Using TCP/IP and named pipes”. Click **Apply**.



- 4 Next, under **SQL Server Browser**, choose the **Startup type** as **Automatic** (use the drop down arrow to select the item). Click **Start** button to immediately start the service. Click **Apply** and **OK**. Area configuration For Services closes.



- 5 Next select Area Configuration for Features. Highlight `xp_cmdshell`. “Enable `xp_cmdshell`” must be set to true. Click **Apply** and **OK** buttons. Close the Configuration Tools.



Appendix E: Schlage SMS Daylight Savings Time Patch

Beginning in the spring of 2007, the start dates and end dates for daylight saving time (DST) will change to comply with the Energy Policy Act of 2005. The Windows Registry and the **Schlage SMS** database should be updated with new settings to reflect the changes to daylight savings.

The program Tzinstall.exe fixes the Windows **Registry Settings** and the **Schlage SMS** database configuration for systems with Windows 2000, XP, and Server 2003 Operating Systems. It is located in the Schlage/Bin directory. Tzinstall.exe will apply the required updates for both the Windows Registry and the **Schlage SMS** database. This allows the **Schlage SMS** software to operate smoothly during the extended daylight saving time. Microsoft is supplying patches for Windows 2003 and Windows XP operating systems which will update the Windows registry.

Note: It is highly recommended that Tzinstall.exe be run on all machines that has **Schlage SMS** installed regardless of the status of your Windows registry.

In the Tzinstall.exe window there are two check boxes (Patch Windows Registry, Patch SMS database) that allow you to choose the updates you may want to perform. If you select both, the program will update the Windows registry and the SMS database and then exit.

Glossary of Terms

A

Access Blocked

Immediately prohibits entry or exit from a reader. This field overrides all area access privileges and activation or expiration dates.

Access under Duress

A feature by which a person entering or exiting an area under threat can signal an alarm to the console. Firmware must be modified to support this option.

Acknowledge

An operation that tells the system that an authorized operator has responded to an alarm event

Activation Date

The fields used to define when a cardholder record or area access permissions will begin.

Advanced Find

A customized search feature used to broaden or narrow a search. It links criteria through the use of Not, And or Or. Searches can be saved for later use

Alarm

A condition that occurs when an attempt at an unauthorized access or other event defined as an alarm has occurred.

Alarm display

Numeric value used to determine the order of appearance on alarm display screen. 1(one) is the highest priority.

Alarm Graphics

Displays real time alarms using maps and icons. Maps represent secured locations. Icons represent alarm devices, overrides and cameras. An icon will flash on the respective map when an alarm becomes active.

Alarm ID

An internal number assigned by the system used to identify the alarm.

Alarm Label

A descriptive name given to the defined alarm.

Alarmed Transaction

An event or condition that represents an abnormal state of the device.

Annotation

A field used to create a prototype and streamline the appearance of a badge. Examples are cardholder image, cardholder field and date. Each type brings a different set of associated fields.

Annotation Control

The graphic items that make up the content of the badge layout.

Antipassback

A process that prevents a card from being presented at the same entry or exit reader twice in a row. Once a card is presented at an entry reader, it must then be presented at an exit reader. This function is used to restrict cardholders from passing their badge to another person for illegal entry.

Area

An Area is any location within a secured building. Areas are collections of readers all of which provide access to the same secured space.

Area Access Permission

Security privileges that are used to grant or deny entry into a secured location. It is further defined by Area, Area Set, Timezone, Expiration Date, Area State and Door Type.

Area Set

An Area Set is a collection of Areas. It has two functions, to organize Areas into logical groups and to provide segmented security on the view of the database records.

Area State

The current mode or status of a secured location such as normal, emergency, lock down or strike.

Area Trees

An alphabetical listing of all the secured locations. **Badge Layout** The customized design and look of the badge which includes background color, images, annotations and size.

Auto Start

Also known as Startup Applications. The **Schlage SMS** applications that can be opened automatically by the System Launcher and do not require operator login. They are Alarm Monitor, Alarm Graphics, CCTV, CIM, History Archiver, System Processor and Universal Triggers.

Automatic Override

A feature that is defined and programmed to change a device's normal state without user intervention. An example is to lock or unlock doors at a specified time.

B

Badge Layout

The customized design and look of a badge. This includes background color, images, annotations and size.

Badge Layout Import Export Utility

Program used to import or export badge layouts outside of the Schlage SMS software to any local or network folder.

Badge Queue

The module responsible for storing badges and dossier reports prior to printing.

Base Report

Pre-defined **Schlage SMS** report that needs only a date and time selection in the Report Launcher module.

Controller

An integrated circuit board connected to the PC by cable, network connection or via telephone lines and a modem. It must be designated as a Master Controller (MC) or Reader Controller (RC).

C

Callback Numbers

Telephone numbers that remote controllers use via a modem to communicate with the PC.

Crop

To trim an image and display only what is inside the rectangle. This feature is found in the Cardholder Image window.

Callback Sets

Groups of controllers that share the same callback telephone numbers.

D

Database

A program that arranges information so that it can be stored, retrieved and manipulated.

Cardholder Categories

Sets of cardholders that share the same access criteria for an area.

DBMS

Database Management System. A program used to create, update and control one or more databases. The **Schlage SMS** uses the Microsoft SQL database management system.

Cardholders

Any entity that is issued a card with an access number.

Delete on Reroute

If the option Delete on Reroute option is selected, when an alarm acknowledgement time has expired, the alarm will be removed from the current workstation and sent to the next workstation in the alarm group sequence.

CIM

The Communication Interface Module is responsible for issuing database changes, gathering and sending information to the boards and storing data in the proper history files. This module should be run on a secured server.

Derived Report

Reports that use the criteria from a **Schlage SMS** Base report to define a sub-report called a Derived Sub-Report. They are identified in the Report Launcher by a yellow lightning bolt.

Device Override

This function permits an operator to control and change the normal operation of readers, relay and contact inputs.

Door Forced Open

This is an alarm transaction programmed on the Alarm Attachment Definition form. It is a condition that occurs when a contact goes into an abnormal state such as from secure to active with no shunt applied.

Door Held Open

An alarm transaction that is generated whenever the DOD shunt timer expires and the door remains open.

Door Open Detect

A contact type programmed on the Contact Definition form.

Door Type

The particular model or kind of door such as pedestrian, vehicular, handicapped or other user defined door.

Dossier Report

A Badge Layout that has been indicated as a dossier thereby allowing the layout to be printed on standard size paper.

Driver

A program used by the operating system to run hardware such as printers, video or sound cards.

DSN (Data Source Name)

The DSN provides connectivity to the database through an ODBC driver

Duplicate Cardholder

An option in the Cardholder Definition program that allows multiple cardholders with the same area access and categories to be entered quickly. Fields from the previous record are copied to the new cardholder record. It will also replicate user defined fields that are marked for duplication.

E

Elevator Control

An integrated system of specific areas, relays, contacts, readers and cardholders that are designated for elevator use.

Encoded ID

A unique numeric value that is required to add a badge to a cardholder record. For instance, a proximity card has a chip programmed with the number. A magnetic stripe card will have the number embedded in the stripe.

Encryption

Data is coded using a special algorithm to provide confidentiality and to prevent hackers from reading private information.

Event Triggers

The actions and functions assigned to devices such as Readers, Relays, and Inputs.

Expiration Date

The fields used to define when a cardholder record or area access permissions will terminate.

Export Cardholder Portraits

A wizard that permits cardholder portraits to be copied outside of the Schlage SMS software to a local or network file location. The user selects the Directory for Export, File Name and Separator.

Expression Builder

A wizard that provides a simple way to create formulas and to link hardcoded text, cardholder fields and/or field separators into one string. Information is encoded in the Magnetic Stripe of a badge. An Annotation Type found in the Badge Annotation Control window of Badge Creation.

F

File Server

A file server (FS) is a robust, high-speed computer with substantial memory, hard disk space and processing power. It maintains all of the system database files and communicates with workstations and the System Processor. Only system administrators should have permission to a file server. Filter A software operation that allows only selected and limited data to appear on the monitor or report.

Filter

A software operation that allows selected and limited data to appear on the monitor or report.

Firmware

Embedded instruction set contained permanently in a chip on the **Schlage SMS** controller board. It acts as a translator between the software and the hardware.

Flashbus MV

One of the imaging systems used by the **Schlage SMS** for image acquisition. A Flashbus MV Video Capture card must be installed on the computer and Flashbus MV must be selected in the software as the Capture Device.

G

GIF

Graphic Interchange Format. A compressed graphic file used on the web. It supports animation but is limited to 256 colors. It is best for logos, line drawing and icons.

Global Antipassback

All boards are synchronized within a Parent / Child system that is utilizing entry and exit readers. When a cardholder is registered at the parent board as "in" (entry) or "out" (exit), updates are sent to all child boards to update the cardholder's antipassback state.

Group Attachment

This is the name given to a collection of Workstations, User Alarm Workstations (operators defined in System Security) and E-Mail Recipients that have been assigned to respond to an alarm. They will receive alarm notification via the Alarm Monitor, Alarm Graphics, E-mail or telephone.

Guest Pass System

An integrated software application that pre schedules visitors and grants temporary access by issuing Access Control Badges and Name Tag Labels. A Web based interface is also available.

H

Hardware

The physical components of a computer.

Hardware Map

An alphabetical listing of all the CIM, Cim Port, controller boards and the devices attached to them.

Holiday Sets

Groups of holidays that share the same holiday access and criteria and works in conjunction with time zones.

Holidays

That may have special access criteria assigned to them. Holiday Sets Groups of holidays that share the same holiday access and criteria and works in conjunction with time zones.

I

Issue Code

The number that represents how many badges have be added to a cardholder record. The first badge is Issue Code 1; the second badge is Issue Code 2 and so on. This is not a required field.

J

JPEG (Joint Picture Experts Group)

A compressed graphic file primarily used for photographs. It supports 16.7 million colors.

L

Log out

An exit procedure performed by a System User at the conclusion of a software session.

Login

A procedure performed at the beginning of a software session by a System User that usually requires entering both a user name and password to gain access to an application.

M

Maintain Aspect Ratio

Image is resized to fit within the annotation box and still keep it's proportions.

Manual Override

The process of predefining commands to cause a change to a device's normal state that in turn can be executed by an operator with a single mouse click. An example would be unlocking specified doors in an emergency.

Mass Access Control Modification

The functionality to mass change access control fields for cardholder records. The fields are Access Blocked, Activation Date, Expiration Date and Controlled Antipassback. This feature is available in the Cardholder Definition module.

MSDE (Microsoft Database Engine)

A database storage engine and query processor that supports transactional desktop applications. It does not have a user interface or tools

Multiple logins

Allows a user to login into several workstations simultaneously.

O

ODBC (Open Database Connectivity)

Developed by Microsoft, this is a standard database access method. Data can be retrieved from any application regardless of the database management system. ODBC uses a driver to translate queries into commands that the DBMS (database management system) understands

Operating System

The main computer program that runs all other applications and is responsible for basic tasks and security. Schlage SMS is compatible with Windows XP and Windows 2000 operating systems.

Operator

A person or entity added in the System Security module with a unique User ID and password. Operator permissions are based on their Security Group. Deleting an active operator places them in retired status. Once a retired operator is deleted, the record is removed from the database.

P

Parent Controller

An intelligent integrated circuit board that controls communication between the **Schlage SMS** system and all Reader controller boards connected to it. Also referred to as the Master Controller(MC).

PDF

Portable Document Format. Software distributed by Adobe Acrobat that allows files to be viewed and printed over several platforms.

PNG

Portable Networks Graphics. Pronounced 'ping', it was developed to surpass GIF and supports 24 bit color. PNG is a compressed graphic file that is widely used on the web.

Portrait Image Enhancer

A feature in the Schlage SMS that presents the user with a selection of 15 images (pictures or signatures). Images can be further enhanced using the Decrease and Increase buttons. It is available as a toolbar and menu option on the Cardholder Image window. It can also be enabled automatically in the System Settings module.

Privileges

Different levels of system access defined in the System Security program for security groups and their operators.

Processor

One of the most important and powerful pieces of computer hardware. It executes numerous commands and instructions.

Program Flash

The application used to download the latest firmware to SRCNX controller boards.

R

RAM, DRAM and SRAM

RAM is an acronym for random access memory. It is a large amount of temporary storage for application and file information. Ram interacts with the operating system and quickly feeds information to the processor. Once the computer shuts down, data is lost from memory. DRAM is Dynamic RAM and is much faster than RAM. DRAM needs to be refreshed thousands of times per second. It accesses information as it needs it, then closes it. SRAM is Static Ram. It is much faster and more expensive than DRAM but does not need to be refreshed. All memory is hardware. RAM chips are mounted on printed circuit boards.

RC (Reader Controller)

The RC is an intelligent hardware device that is capable of making decisions at the local level. The RC controls card reader, keypad, relay and contact input activity.

Reader Template

This is used to designate fields and values that will be duplicated. A reader is assigned as a Reader Template when additional readers will use the same or similar relay, contact, event trigger and override information.

Reload SP Memory

Command that will immediately send alarm records and changes to the System Processor.

REX (Request to exit)

A contact type programmed on the Contact Definition window.

RI (Reader Interface)

The RI is a physical hardware device that reads the access card. It connects the Read Head to the system controller board. The RI will support one Read Head, one or two relays and 7 contact inputs

S

Security Group

A collection of operators that share the same security permissions

Service Pack

Security fixes and program updates issued by companies that develop applications. Window updates are located at <http://windowsupdate.microsoft.com>

Site Codes

Unique numerical values that are pre programmed into access cards and assigned to Areas. They are used to grant or deny access. Site codes are stored at the Reader level and permit access when an HC11 reader is in Degraded Mode.

Software

Programs that run on a computer

SP (System Processor)

The SP directs alarms and transactions to their proper destination. It acknowledges, secures and tracks alarms then logs them to the history file

SQL (Structured Query Language)

A powerful, relational database capable of handling large-scale applications

SRCNX

Schlage Reader Controller Next Generation. This term refers to one of Schlage controller board models.

SRINX

Schlage Reader Interface Next Generation. Connects the read head to the controller board.

Stamped ID

An internal company defined numbering system that is sometimes displayed on the back of a badge. Stamped ID is not a required field to add a badge

Status Levels

Access Control System version 5.X, no longer uses Status Levels; they have been replaced by Area Access Permissions. Status Levels were security privileges that allowed cardholder access permissions to selected readers during specific timezones.

SVTR

Schlage Video Transaction Retrieval. This module provides interface and retrieval of digitally stored video of Schlage Security Management System transactions.

System Manager

This module is used to define, edit, attach and delete devices, areas, area sets, timezones, holidays, site codes and callback numbers.

System Software

The **Schlage SMS** software is comprised of over thirty-plus integrated high tech security access programs. It is a sophisticated and intelligent security system offering a wide array of features and functions that control and report on access, alarm and security activity.

T**TCP/IP**

Transfer Control Protocol / Internet Protocol. A common language (protocol) used by computers to communicate on the internet and with other computers.

Timezone Intervals

Segments of time used to determine when and for how long a cardholder should have access or a device to be activated or deactivated in any given Area.

Timezone Tree

An alphabetical listing of all timezones that have been defined within the system.

Transaction Monitor

A module in the **Schlage SMS** that is used to view the system activity in real time and access previous transactions, transaction filters and dial up controllers.

Transparency

Used on badges in conjunction with cardholder images, static picture or signatures. When used, the background shade becomes invisible.

U

UDF (User Defined Fields)

Customized fields that can be added to Cardholder and Guest records

Universal Trigger

A universal trigger enables a series of actions in response to a specified event to be sent across any or all CIMs and attached devices throughout the system.

Unretire Credential

A credential that has been reactivated from retired status to active status

User Alarm Workstation

An alarm monitor that has been defined and assigned to a specific operator with a single User ID. Operators are added in the System Security module.

UTC (Universal Time, Coordinated)

This is also known as Greenwich Mean Time (GMT)

V

Virus

A program intentionally written to cause damage to a computer, it's programs and operating system. A virus is commonly sent in the form of e-mail attachments and can spread rapidly to other computers

W

WAV (Wave File)

A file used by computers to play recorded sounds such as music or instructions. The file name extension is .wav

Wildcard

A value entered in a query field that represents any other value and used when an exact value is not known. In the **Schlage SMS** software, a user can type the % (percent sign) before or after their search text. Wildcards are formally known as Metacharacters.

Wizard

A simple feature that prompts the user for necessary information then carries out a complex task automatically.

Workstation

A computer used by operators to access software applications, to input data, retrieve transaction information and alarms. Workstations are generally networked to a server.

Worm

A malicious program that is introduced into a computer and works similar to a virus.

Write Privileges

An operator is permitted to view and make additions, modifications and/ or delete records.

Index

A

- A brief note on permissions • 202
- Access Blocked • 589
- Access Control • 486
 - Enable Access Control Requirement • 486
- Access Denied Transactions • 263
- Access Property Values • 465
- Access under Duress • 589
- Access Under Duress Transactions • 114
- Accessing other applications from Transaction Monitor • 348
- Accessing the Application • 258
- Acknowledge • 589
- Acknowledged and not secured • 284
- Acknowledged and Not Secured • 284
- Acknowledging Alarms • 284, 290, 327
- Acronym • 22
- Activation and Expiration Tab • 515
- Activation Date • 589
- Activation Expiration • 515
- Active Alarms • 283
- Active Badge Options • 147
- Active Credential Options • 147
- Active Online Credentials • 146
- Add a Guest • 500
- Add a new Cardholder • 138
- Add a new Cardholder (Method 2) • 169
- Add an Operator • 197, 198
- Add and Authorize a Guest • 507
- Add Card Formats in the System • 193
- Add New Cardholders • 138
- Add, Authorize and Sign In a Guest • 507
- Add, Sign In and Authorize a Guest • 507
- Adding a Card Format in the System • 192
- Adding a new group • 267
- Adding a Property • 463
- Adding Alarm Labels • 317
- Adding an Access Plan • 462
- Adding an Alarm Label • 265
- Adding Application to the Start up • 203
- Adding Application to the Start up Tab • 203
- Adding Applications to the Launcher • 202
- Adding applications to the Launcher Group • 43
- Adding applications to the Start up tab • 203
- Adding applications to the System Launcher • 202
- Adding cardholder Badges to the Queue • 232
- Adding Cardholder Badges to the Queue • 232
- Adding Credentials to the Lock • 123
- Adding email addresses • 169
- Adding e-mail addresses • 243
- Adding E-mail Addresses • 169, 243
- Adding Image • 499
- Adding Portraits to a Badge or a Label • 499
- Adding Security Groups • 197
- Adding Signature • 499
- Adding Signature to the Badge • 505
- Adding Workstations • 268
- Additional Annotation Design features • 225
- Additional Annotation Design Features • 225
- Advance Find • 306

- Advanced Find • 234, 245, 260, 274, 331, 338, 368, 512, 589
- Advanced Importer • 545
- Advanced Search Settings • 60
- Alarm • 589
- Alarm Acknowledgement • 324
- Alarm Attachments • 272
- Alarm Definition • 264, 285, 290, 327
- Alarm display • 589
- Alarm Graphics • 589
- Alarm Graphics Client
 - Alarm Acknowledgement • 324
 - Alarm Notification • 323
 - Pre-defined Alarm Comments • 329
 - View Cardholder Image • 330
- Alarm Graphics-Client • 322
- Alarm Graphics-Editor • 312
- Alarm Graphics-Settings • 308
- Alarm ID • 589
- Alarm Label • 589
- Alarm Label Definition • 265
- Alarm Monitor • 282, 322
 - Acknowledging Alarms • 284
 - Executing Override Tasks • 288
 - Minimize Alarm Monitor • 292
 - Receiving Video of Alarms • 288
 - Viewing and Editing Cardholder Information • 286
 - Viewing Previous Alarms • 287
- Alarm Notification • 323
- Alarm State Builder • 300
- Alarm State Definition • 301
- Alarm Types • 296
- Alarmed Transaction • 589
- Animation Script Builder • 302
- Animation Template Definition • 302
- Annotation • 589
- Annotation Control • 590
- Annotation Design Features • 225
- Antipass Back • 108
- Antipassback • 590
- Appendix A
 - MSSQL 2000 Backup and Restore Procedures • 557
- Appendix B
 - File Space Monitor • 563
- Appendix C
 - Database Maintenance Utility • 575
- Appendix D
 - MSSQL 2005 Server Configuration Settings • 585
- Appendix E
 - Schlage SMS Daylight Savings Time Patch • 588
- Archive History • 351
- Area • 590
- Area Access • 24, 76, 143, 515
- Area Access Commands • 552
- Area Access Permission • 590
- Area Count Tracking • 256
- Area Definition • 250
- Area Set • 590
- Area Set Permissions • 205
- Area State • 590
- Area States and Door Types • 62
- Area Trees • 590
- Areas and Area Sets • 75, 256
- Areas, cardholders and readers • 23

Arranging the icons of a Group • 44

Assigning Access Rights to a Campus Lock • 469

Assigning Areas and Area Sets • 142

Assigning Areas, Area Sets • 142

Assigning security privileges • 196, 204

Assigning Security Privileges • 204

Attaching a Transaction to a Filter • 336

Attaching Groups with Labels • 270

Attaching Override Sets, Tasks and Camera Control • 320

Attaching Tasks to Sets • 356

Audit trail • 447

Audit Trail Report • 408

Audit Trail-Settings • 405

Authorization

- Authorization Option See glossary of terms also. • 487

Authorization options • 487

Authorization Options • 487

Authorize a Guest • 505

Authorize a Pending Guest • 505

Auto Detect Scan • 500

Auto Sign-out options • 495

Auto Start • 590

Auto unlock Offline Locks • 367

Auto-load the saved Monitor • 343

Automatic Override • 590

Automatic Override Actions • 366

Automatic Override Definition • 363

Automatic Page Feed Detection • 500

Automatically create CM Lock Credential • 148

Automatically generating Credentials • 164

B

Backup Options • 55

Backup SQL Database • 557

Badge Creation • 215

Badge Criteria • 514

Badge Default Print Options • 63

Badge Layout • 590

Badge Layout Import Export Utility • 590

Badge Layout Permissions • 212

Badge Printing • 488

- Badge Technology • 488

Badge Printing Defaults • 63

Badge Printing

- Default Badge Layout • 488

Badge Queue • 230, 590

Badge Queue Definition • 231

Badge Technology • 488

Badging • 488

Bar Code Settings • 221

Base Report • 591

Boolean • 237

Border Setting / Date and Time Format Options • 223

Button combination functions • 480

C

Callback Numbers • 591

Callback Numbers and Callback Sets • 85

Callback Sets • 591

Campus Lock Credential Definition • 156

Campus Lock Settings • 53, 65, 460

Campus Locks • 459

Card Access Values • 156, 158

Card Alarms • 296

- Card Format Editor • 180
- Card Format Editor main window • 181
- Card Format Editor usage scenarios • 184
- Cardholder Categories • 84, 591
- Cardholder Category • 213
- Cardholder Category Permissions • 212
- Cardholder Definition • 55, 137
 - Add New Cardholders • 138
 - Area Access • 143
 - Assigning Areas, Area Sets • 142
- Cardholder Definition Default Expiration Date • 55
- Cardholder Definitions
 - Adding E-mail Addresses • 169
 - Advanced Find Feature • 174
 - Assigning Areas, Area Sets • 142
 - Badge Definition
- Active Badge Options • 147
- Add Badges • 146
- Generating Badges Automatically • 164
 - Badge Definitions
- Retire Badges • 148
 - Cardholder Search Wizard • 174
 - Delete Cardholders • 170
- Delete a Single Cardholder record • 170
- Multiple Cardholder Deletions • 171
 - Deleting E-mail Addresses • 170
 - Duplicate Cardholder Information • 169
 - Export Cardholder Portraits • 171
 - Generating Badges Automatically • 164
 - Portrait Capture • 144
 - Printing Reports • 172
 - Use of Wildcards • 177
- Cardholder Field Permissions • 212, 214
- Cardholder Search • 174
- Cardholder with Access to Area • 80
- Cardholders • 591
- Categories • 177
- CCTV • 470
- CCTV Camera Control • 470
- Changing the password for accessing UpLink Configuration • 443
- CIM • 412, 591
- CIM and SP Status Messages • 351
- CIM Start up screen • 416
- CIM to RC Communications • 351
- Closing Date and Time Delays and accessing the Help file • 449
- Closing Offline Lock Interface • 439
- CM lock credential definition • 148
- CM Lock Credential Definition • 148
- Color codes for Com Port Status • 416
- Color Schemes • 498
- Column Name Definition • 410
- Com Port Expansion • 417
- COM Port Expansion File Menu • 417
- Commands for adding and deleting cardholders • 549
- Commands for adding, retiring, and deleting credentials • 550
- Communication Alarms • 297
- Communication Status Messages • 430
- Configuration • 459, 460
- Configure OLI to work with Windows Sync Application • 454
- Configuring a Portrait Monitor Workstation • 259
- Configuring Transactions, Devices, Alarms etc. • 475

- Connecting to Panels via Dial-up • 347
- Contact Alarms • 297
- Contact Definitions • 112
- Contact Point Supervision using Parallel and Series Resistors • 113
- Contacts • 491
- Controller • 591
- Controller Update • 428
- Copying Areas to Area Sets • 79
- Create a New Map • 313
- Creating a Filter • 336
- Creating a Filter Set • 335
- Creating a new report • 401
- Creating a new Report Group • 396
- Creating a New Report Group • 396
- Creating a new Schedule • 392
- Creating a new Sub Report • 396, 401
- Creating a New Sub Report • 396, 401
- Creating a new User Definable Field • 236
- Creating a New User Definable Field • 236
- Creating a Shift • 253
- Creating Evacuation Reports • 403
- Creating Group Attachments • 267
- Creating Guest Records • 498
- Creating icons and animated graphics • 315
- Creating Icons and Animated Graphics • 315
- Creating Launcher Groups • 42
- Creating Teams • 255
- Credential Criteria • 514
- Credential Definition • 144
- Credential Import Choices • 542
- Credential Insert Full Automation Mode • 166
- Credential Insert Partial Automation Mode • 165
- Credential Issuance Settings • 60

- Credentials • 24
- Crop • 591
- Current Workstation Offline Credential Settings • 68, 71
- Current Workstation Settings • 67
- Customer support • 47
- Customize the Transaction Code • 341
- Customizing the Transaction Monitor • 341
- Customizing Transaction Codes • 334, 341

D

- Data file utilization in Schlage SMS • 563
- Data Type Definitions • 237
- Database • 591
- Database Connection • 51
- Database maintenance procedures for restoring the database • 581
- Datatype Definitions • 237
- Date & Time & Delays • 448
- Date & Time Delays • 448
- DBMS • 591
- Default Label layout • 489
- Default Printers • 64
- Default Programs and Devices • 55
- Default Queues • 64
- Default State of an Icon • 330
- Default user ID and password • 43
- Define a Reader • 106
- Define a Relay • 114
- Define a Two Person Area - Schedules or Team • 256
- Define a Workstation • 86
- Define Areas • 376
- Define Automatic Override Tasks • 365
- Define Campus Locks • 130

- Define CIM • 87
- Define CIM Port • 88
- Define CM Locks • 119
- Define Contacts • 384
- Define Controllers • 89, 377
- Define Launcher Items • 202
- Define Login Requirements • 200
- Define Offline Lock Access • 154
- Define Readers • 251, 379
- Define Relays • 383
- Define Settings • 485
- Define SSRC • 91
- Define SSRC-300 • 96
- Define SSRC-400 • 101
- Defining a Location • 493
- Defining a new badge layout • 216
- Defining a new Badge Layout • 216
- Defining a new Magstripe Format • 189
- Defining a Template • 486
- Defining a Wiegand Format • 193
- Defining a workstation • 494
- Defining a Workstation • 494
- Defining Access for Campus Locks • 462
- Defining Access Plan Properties • 463
- Defining Access Plans for Campus Locks • 462
- Defining Alarms • 265
- Defining annotations for a new Badge Layout • 218
- Defining Annotations for the New Badge Layout • 218
- Defining Area Sets • 76
- Defining Areas • 77
- Defining Campus Locks • 467
- Defining Filters • 335
- Defining Manual Override Actions • 356
- Defining Manual Override Sets • 354
- Defining Manual Override Tasks • 355
- Defining User Types • 133, 466
- Definition of fields in the COM Port Expansion window • 418
- Degraded Mode • 112
- Delete a Guest Record • 511
- Delete a Schedule • 394
- Delete Cardholders • 170
- Delete on Reroute • 591
- Deleting a Lockdown • 84
- Deleting a Record • 132
- Deleting a single cardholder record • 170
- Deleting a Sub Report • 404
- Deleting a Sub-report • 404
- Deleting an Access Plan • 463
- Deleting applications from user created groups • 44
- Deleting Areas • 81
- Deleting email addresses • 170
- Deleting E-mail Addresses • 170
- Deleting Offline Lock Access • 154
- Deleting records • 244
- Deleting Records • 244
- Deleting Reports • 397
- Derived Report • 591
- Description of Annotation types • 220
- Description of Annotation Types • 220
- Description of tabs • 511
- Designing a New Badge Layout • 216
- Designing Filters • 335
- Detail View • 262
- Device Control • 351

Device Override • 592
Device Status • 132
DFO† HO Alarm • 277
Door Forced Open • 592
Door Forced Open/Door Held Open Alarms • 277
Door Forced Open\Door Held Open Alarms • 277
Door Held Open • 592
Door Open Detect • 592
Door Type • 592
Dossier Default Print Options • 63
Dossier Report • 592
Download Sync Program • 452
Download/Update Status Messages • 351
Driver • 592
Driver' s License Scanner • 500
DSN (Data Source Name) • 592
Duplicate Cardholder • 592
Duplicate Cardholder Information • 169
Duplicate CM Lock Definition • 125, 126
Duplicating a Badge Layout • 218

E

Edit • 357
Edit a Schedule • 394
Edit Menu • 472
Edit options • 423
Edit Options • 242
Editing • 275
Editing a Badge Layout • 218
Editing a Base Report • 396
Editing a Magstripe Template • 131
Editing a Map • 321
Editing a Sub Report • 403
Editing a Sub-report • 403
Editing an Access Plan • 463
Editing an Alarm Label • 267
Editing an Existing Mapping • 249
Editing and deleting Report Groups • 396
Editing and Deleting Report Groups • 396
Editing Annotations • 225
Editing Card Formats • 188
Editing CM Lock Credentials • 148
Editing CM Lock Definition • 124
Editing Filter Definitions • 337
Editing Lockdowns • 84
Editing Magstripe Options • 218
Editing Online Credential information • 167
Editing Online Credential Information • 167
Editing Queues • 233
Editing records • 133, 244
Editing Records • 244
Editing the Guest Information • 510
Editing the Queue • 233
Editing Timezone Intervals for CM Locks • 125
Editing Transaction Monitors • 343
Edting Offline Credentials • 148
Elevator Control • 375, 592
Elevator Control Setup • 375
E-Mail • 490
E-mail Address Editor • 243
E-Mail Enabled Features • 490
E-Mail Recipient • 268
E-Mail Server Settings • 491
Enable E-Mail • 500
Encoded ID • 592

Encoded ID Settings • 489
Encoding a Credential • 156
Encryption • 592
End Report • 409
Enrollment Reader Setting • 59
Entry and Exit Under Duress • 116
Error messages • 439, 450
Event Triggers • 116, 592
Example for an Automatic Override • 366
Example for An Automatic Override • 366
Examples of commonly used MRO procedures • 357
Examples of Schlage SMS in the field • 567
Executing Override Tasks • 288
Executing Override Tasks and Sets • 357
Exiting Alarm Definitions • 276
Exiting CIM • 419
Exiting Launcher • 46
Exiting View SP Status Application • 427
Expiration Date • 593
Expiration Indicators • 54
Explanation of File Space Monitor Program Items • 565
Explanation of terminology • 565
Export Cardholder Portraits • 171, 593
Exporting Badge Layout • 229
Exporting Badge Layouts • 229
Exporting Cardholder Portraits • 171
Exporting Cardholder Search Results • 135
Exporting Data • 148
Expression Builder • 593

F

File • 304

File Menu • 472
File menu options • 231
File Menu options • 231
File Server • 593
Files and documents included in this package • 574
Filter • 593
Filter Permissions • 205
Filtering Transactions • 345
Firmware • 593
Flashbus MV • 593

G

General Image Capture Settings • 56, 57
General Setting • 485
General Settings • 54, 395
generate an audit trail report • 411
Generating an Audit Trait Report • 409
Generating Credentials Automatically • 164
Generating programming files • 439
Generating Programming Files • 439
GIF • 593
Global Antipassback • 593
Global Offline Credential Settings • 68
Global Settings • 65, 495
Group Attachment • 267, 593
Group Attachments • 267
Grouping Structure - Area Sets and Cardholder Categories • 23
Guest Alarms • 299
Guest Fields • 513
Guest Pass Locations • 493
Guest Pass Settings • 484
Guest Pass System • 55, 497, 594

Guest Pass System Installation (only applicable to Schlage SMS Premier users) • 41

Guest Pass Transaction • 351

GVTR Camera Control • 474

H

Hardware • 594

Hardware Connection Diagram • 386

Hardware Definitions • 86

Hardware Map • 594

Hardware Requirements • 500

Holiday Sets • 594

Holidays • 594

Holidays and Holiday Sets • 82

Hours of operation • 47

How to Alarm an Access Under Duress Transactions • 116

How to resolve problems with UpLink • 450

I

Icon - Views • 44

Identifying existing credential formats • 185

Image Handling • 56

Image Verification • 490

Implications • 280

Import Options • 540

Import Settings • 548

Imported Data Types • 523

Importing a Badge Layout • 228

Importing and Exporting Badge Layouts • 227

Importing LockLink 7 Database • 531

Importing LockLink Express Database • 525

Information Box Setting • 311

Information section • 430

Ingersoll Rand Copyright Notice • 1

Inserting icons on Maps • 315

Inserting Icons on Maps • 315

Installation and Getting Started • 29

Installation and set-up • 577

Installation instructions • 30

Instruction to Register a Programming Credential • 66, 461

Instructions • 491

Integer • 237

Invalid Transactions for Elevator Control • 385

IR Viewer • 478

Issue Code • 594

J

JPEG (Joint Picture Experts Group) • 594

L

Label Printing • 489

 Default Label layout • 489

 Label Printer • 489

Launcher Group Properties • 45

Launcher Items • 202

Launching a Report • 400

Launching the Portrait Monitor • 262

License Field Cross Reference • 519

Limitations • 522

Linking source columns with Cardholder fields • 541

Location

 Add, Delete, Edit and Select Location • 493

Locations • 515

Lock forever • 360

Lockdowns • 83

LockLink Import Wizard • 521

Log file • 543

Log out • 594
Logging out of the system • 47
Login • 594
Login Requirement Definitions • 200
Login Requirements • 200
Login Requirements Definitions • 200
Lookup List • 237

M

Magstripe Template • 184
Magstripe Template Definition • 130
Main screen view • 413
Maintain Aspect Ratio • 594
Make a Pending Guest Record • 511
Manual operation of the Database Maintenance Utility • 580
Manual operation to restore a backup of the SchlageSQL • 581
Manual Override • 594
Manual Overrides • 354
Manual Overrides and Trigger Events • 370
Manual Overrides within Portrait Monitor • 263
Mapping • 247, 519
Mass Access Control Modification • 594
Mass Insert • 244
Massive access control modification for cardholders • 168
Massive Access Control Modification for Cardholders • 168
Maximum Value • 489
Menu options • 303, 373
Menu Options • 472
Min screen • 421
Minimize Alarm Monitor • 292
Minimum PC requirements • 29

Modify Area Access • 143
Modifying and Deleting (Retiring) Operators • 200
Modifying and deleting operators • 200
Modifying Animation Scripts • 303
Modifying Launcher Items • 203
Momentary lock • 359
Momentary unlock • 357
MSDE (Microsoft Database Engine) • 595
Multiple cardholder deletions • 171
Multiple Cardholder Deletions • 171
Multiple logins • 595

N

Navigation View Settings • 309
Navigation/Tool bar options • 367
New cardholder wizard • 139
New Cardholder Wizard • 139
New Method • 279
New User Definable Field • 236
Notes on associated Transaction Sets • 276
Notes on issuing badges to cardholders and printing • 226
Notes on Issuing Badges to Cardholders and Printing • 226
Notes on upgrading the firmware • 433
Notes on Windows Vista/Windows 7 Install • 37

O

ODBC (Open Database Connectivity) • 595
Offline Credential Settings • 68
Offline Credentials • 148
Offline Lock Interface • 434
Offline Lock Transactions • 299
Old Method • 277

- On Watch List • 516
- Online and Offline Access Control • 25
- Online Credential Options and Pin Calculator • 59
- Operating System • 595
- Operation performed by the SQL Agent • 579
- Operator • 595
- Operator Alarms • 298
- Operator's requirements • 29
- Option 2 • 507
- Option 3 • 507
- Options • 276, 295, 305, 346, 413
- Other • 492
- Override Sets and Reports • 205, 214
- Overview • 180, 258, 497

P

- Parent Controller • 595
- Pausing Transactions • 263, 343
- PDF • 595
- Person with Disability • 500
- Pin Calculator Settings • 61
- Playback Viewer – save an MJPEG file • 482
- Playback Viewer screen explanation • 479
- Playing video file of a Transaction • 345
- PNG • 595
- Pop-up on Transaction • 346
- Portrait Capture • 144, 490
 - Adding Image to a Badge or a Label • 499
 - Editing an Image • 499
 - Flash Bus MV • 499
 - Image Verification • 490
 - Portrait Settings
- Portrait Capture Device • 494

- TWAIN Device • 499
- Portrait Image Enhancer • 595
- Portrait Monitor • 261
- Portrait Monitor Control • 258
- Portrait Monitor Search Wizard • 259
- Portrait Monitor-Settings • 258
- Pre-defined Alarm Comments • 284, 329
- Preface • 23
- Pre-requisites for importing a LockLink 7 Database • 531
- Pre-requisites for importing a LockLink Express file • 525
- Previous Alarms • 293
- Previous Transactions • 349
- Print Alarm Screen • 292
- Printing a Exporting Reports • 401
- Printing Badges • 232
- Printing Dossier Reports • 172
- Printing Reports • 172
- Printing the Alarm screen • 292
- Privileges • 595
- Processor • 595
- Program a lock for the first time: • 456
- Program Flash • 431, 596
- Program Lock • 456
- Program Locks • 444
- Programming • 444, 470
- Programming a Trigger Event • 372
- Programming Automatic Overrides • 364
- Programming Automatic Overrides for Campus Locks • 469
- Programming Manual Overrides • 354, 366
- Programming the Locks • 439
- PTZ Panel • 291, 328

Q

Quick Launch feature • 400

Quick Launch Feature • 400

R

RAM, DRAM and SRAM • 596

RC (Reader Controller) • 596

Reader Template • 108, 596

Reader Types and Tracking Issues • 382

Rearranging and sorting column titles • 411

Rearranging and sorting Column Titles • 411

Rearranging Launcher Group tabs • 46

Receiving video of alarms • 286, 288, 325

Recently Launched Applications • 46

Refresh • 132

Refresh Report • 409

Registry Editor • 48

Relay Alarms • 297

Relay Transactions • 351

Reload SP Memory • 596

Renaming a Launcher Group • 44

Replacement Credential • 160

Replacing a Card • 156

Report Database Connection • 52

Report Groups and Sub Reports • 395, 396

Report Launcher • 398

Report Launcher Settings • 395

Report Scheduler • 389, 392

Report Scheduler Service • 390

Report Scheduler Service Manager • 391

Requirements • 432

Reset and Update • 429

Reset devices • 359

Reset Guests to Pending • 509

Reset lock • 361

Reset momentary lock • 360

Reset momentary unlock • 358

Resetting a Controller • 429

Resolution • 564

Restore SQL Database • 559

Restoring Archived History • 404

Retire Credentials • 167

Review screen • 543

REX (Request to exit) • 596

RI (Reader Interface) • 596

Room Change • 156, 161

RR Transactions • 299

Run Report • 409

Running a Report • 294

Running a report of Alarms • 294

S

Save an AVI file • 481

Saving a MJPEG file • 482

Saving a video clip to a file • 480

Saving new configuration settings • 443

Saving Transaction Monitors • 342

Scan • 500

Schedule Preferences • 571

Scheduled Updated for Controllers • 90

Schlage GUI Importer • 538

Schlage SMS field problems and solutions • 573

Schlage SMS Image Settings • 56

Schlage SMS Levels • 27

Schlage SMS Select System Security • 195

Schlage SMS Signature Settings • 58

Search • 134, 244, 274, 304, 337, 367, 512

Search for a Guest • 512, 513
Search for Badge Queues • 233
Security Group • 596
Security Tour System Transactions • 351, 353
Selecting a Cardholder • 177
Selecting a Transaction Group • 342
Serial Port Communication Test • 471
Service Pack • 596
Set Up Sync Program • 453
Setting dates • 411
Setting up maps and icons • 313
Setting up Maps and Icons • 313
Setting up Schlage Enrollment Reader • 145, 149, 150, 182
Settings • 48, 406, 412
Shutdown/start -up main screen • 416
Sign In a Guest • 506, 508
Sign In Question • 487
Sign Out a Guest • 508
Signature Capture • 144
SIONX 24 wiring Instructions • 386
Site Codes • 596
Site Codes and Site Code Sets • 85
Software • 596
SP (System Processor) • 597
SP Settings • 422
SQL (Structured Query Language) • 597
SRCNX • 597
SRINX • 597
Stamped ID • 597
Starting SP • 420
Starting the CIM • 412
Starting the Portrait Monitor • 261
Status Levels • 597

Status Messages • 415
Step 1 • 564
Step 2 • 564
Step 3 • 564
Step 4 - Backup Database • 567
Step 5 • 567
Steps for importing a LockLink 7 database • 532
Steps for Importing a LockLink Express File • 525
Steps for running the Importer • 546
Steps to insert a New Icon • 315
Steps to Insert a New Icon • 315
String • 237
Supervisor Access • 257
Supported commands • 549
SVTR • 286, 288, 290, 325, 327, 474, 597
Sync Program Configuration • 452
System Alarms • 298
System Information • 49, 415
System Launcher • 29, 42, 53, 72, 420
System Manager • 55, 72, 597
System Manager Permissions • 206
System Overview • 23
System Processes • 50
System Processor • 420
System requirements for IR Viewer • 478
System Requirements for IR Viewer • 478
System Security • 194
System Settings • 53
System Software • 597

T

Table Refresh Timer • 492
TCP/IP • 597

Team Definition • 252
Temporary Card • 156
Temporary Credential • 161
Text Styles • 222
Timed Override Task and Set • 356, 357, 362
Timezone Intervals • 74, 597
Timezone Tree • 597
Tool bar • 276, 295
Tool bar icons • 350, 414
Toolbar • 305
Toolbar Icons • 472
Tools Menu • 472
Transaction Codes Editor • 333
Transaction Filters • 335
Transaction Monitor • 340, 598
Transaction type definitions • 351
Transaction Type Definitions • 351
Transactions • 24
Transparency • 598
Two Person Rule • 77, 250
Typographical Conventions • 21

U

UDF (User Defined Fields) • 598
UDF Cross Reference • 246
Understanding a Report • 410
Universal Trigger • 598
Universal Triggers • 369
Unlock forever • 358
Unretire Credential • 598
Update a lock • 457
Update the program files on the PDA • 456
Update the SMS files • 458
Updating a controller • 429, 430
Updating controller memory • 432
Upgrade instructions • 38
Uplink configuration • 440
Uplink Configuration • 440
Use of wildcard • 177
Use of Wildcard • 307, 331
Use of Wildcards • 513
User Alarm Workstation • 598
User Defined Field Template • 237
User Defined Fields • 235
UTC (Universal Time, Coordinated) • 598
Utilities • 449

V

Various selections and extended settings • 441
Video Compression dialog • 481
View • 134, 172
View Access Records • 124
View Alarm Comments • 295
View Cardholder Image • 330
View log file • 424
View menu • 425
View Previous Alarms
 Alarm Types • 296
 Communications Alarms • 297
 Contact Alarms • 297
 Relay Alarms • 297
 Running a Report • 294
 View Alarm Comments • 295
View Settings • 413
View tab displays • 361
Viewing a Badge Layout • 233
Viewing a double-sided badge • 226
Viewing a Double-Sided Badge • 226

- Viewing and editing Cardholder information • 286
- Viewing Attachments • 199
- Viewing Badge Layout • 233
- Viewing Cardholder Portrait and Signature • 344
- Viewing log files • 438
- Viewing Log Files • 438
- Viewing Previous Alarms • 287
- Viewing Previous Transactions • 348
- Viewing the main screen • 273
- Virus • 598
- Void credential • 164
- Void Credential • 156

W

- Warnings and Error Messages • 536
- WAV (Wave File) • 598
- Wildcard • 598
- Wizard • 598
- Working with Alarm Graphics Editor • 313
- Working with Alarm Monitor • 283
- Working with Animation Builder • 301
- Working with Automatic Overrides • 364
- Working with Badge Queue • 230, 231
- Working with Cardholder Definition • 138
- Working with Controller Update Utility • 429
- Working with GUI Importer • 539
- Working with IR Viewer • 479
- Working with Offline Lock Interface • 435
- Working with Portrait Monitor • 262
- Working with Previous Alarms • 294
- Working with Previous Transactions • 350
- Working with Report Launcher • 399
- Working With Schlage Utility Software (SUS) • 452
- Working with SVTR Camera Control • 291, 328, 474
- Working with System Manager • 73
- Working with System Security • 196, 197
- Working with the Portrait Monitor • 262
- Working with the System Security • 197
- Working with the Transaction Monitor • 341
 - Auto-load the Saved Monitor • 343
 - Customize the Transaction Code • 341
 - Customizing the Transaction Monitor • 341
 - Defining a Monitor • 341
 - Editing Transaction Monitors • 343
 - Filtering Transactions • 345
 - Pausing Transactions • 343
 - Popup on Transaction • 346
- Working with the Transaction MonitorSaving Transaction Monitors • 342
- Working with Transaction Monitor • 341
- Working with UDF Cross Reference • 246
- Working with UDF Editor • 235
- Working with Uplink • 440
- Workstation • 598
- Workstation Type column. E-Mail Recipient • 268
- Workstations • 268
- Workstations, alarm operators and email recipients • 268
- Worm • 599
- Write Privileges • 599



Ingersoll Rand's Security Technologies Sector is a leading global provider of products and services that make environments safe, secure and productive. The sector's market-leading products include electronic and biometric access-control systems; time-and-attendance and personnel scheduling systems; mechanical locks; portable security; door closers, exit devices, architectural hardware, and steel doors and frames; and other technologies and services for global security markets.

866-322-1237

www.schlage.com www.ingersollrand.com